

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-031130

(43)Date of publication of application : 02.02.1999

(51)Int.Cl.

G06F 15/00
G09C 1/00
H04L 9/32

(21)Application number : 09-184866

(71)Applicant : FUJI XEROX CO LTD

(22)Date of filing : 10.07.1997

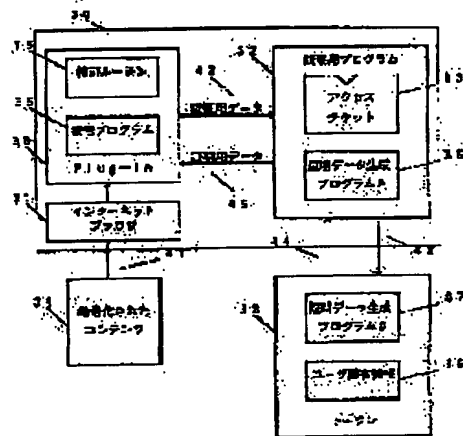
(72)Inventor : KONO KENJI
NAKAGAKI JUHEI
KOJIMA SHUNICHI

(54) SERVICE PROVIDING DEVICE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide the utilization of service only to a user who has a legal right, minimizing the burden on the user and a service provider.

SOLUTION: When a plug-in 38 of an internet browser 31 is started, a verification program 15 in the plug-in 38 is started, communicates with a program 32 for certification and performs user authentication. A certification data generation program A36 of the program 32 cooperates with a certification data generation program B37 in a token 33, calculates based on a user inherent information 16 and an access ticket 13 and communicates with the program 15 in the plug-in 38 based on the calculation. As the result of the communication, the success of authentication by the program 15 is limited to only when the three of the user inherent information, the access ticket and enciphered contents correctly correspond with one another.



LEGAL STATUS

[Date of request for examination] 13.06.2002

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-31130

(43) 公開日 平成11年(1999) 2月2日

(51) Int.Cl. ⁸	識別記号	F I
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00 3 3 0 B
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00 6 4 0 B
H 0 4 L 9/32		H 0 4 L 9/00 6 7 5 B

審査請求 未請求 請求項の数21 O L (全 44 頁)

(21) 出願番号 特願平9-184868

(22) 出願日 平成9年(1997) 7月10日

(71) 出願人 000005496

富士ゼロックス株式会社

東京都港区赤坂二丁目17番22号

(72) 発明者 河野 健二

神奈川県足柄上郡中井町境430 グリーン

テクノikai 富士ゼロックス株式会社内

(72) 発明者 中垣 寿平

神奈川県足柄上郡中井町境430 グリーン

テクノikai 富士ゼロックス株式会社内

(72) 発明者 小島 俊一

神奈川県足柄上郡中井町境430 グリーン

テクノikai 富士ゼロックス株式会社内

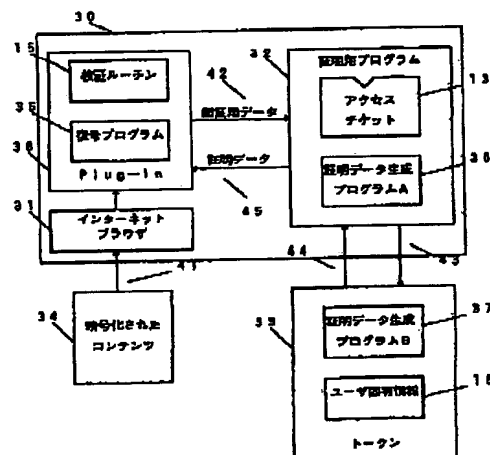
(74) 代理人 弁理士 澤田 俊夫

(54) 【発明の名称】 サービス提供装置

(57) 【要約】

【課題】 ユーザおよびサービス提供者の負担を最小限に押さえながら、サービスの利用を正当な権利を有するユーザにのみ提供する。

【解決手段】 インターネットブラウザ31のプラグイン38が起動すると、プラグイン38中の検証プログラム15が起動し、証明用プログラム32と通信してユーザ認証を行う。証明用プログラム32の証明データ生成プログラムA36は、トークン33中の証明データ生成プログラムB37と協調して、ユーザ固有情報16とアクセスチケット13とに基づいて計算を行い、その計算に基づいてプラグイン38中の検証プログラム15と通信を行う。通信の結果、検証プログラム15による認証が成功するのは、ユーザ固有情報と、アクセスチケットと、暗号化されたコンテンツとの3つが正しく対応している場合に限られる。



(2)

特開平11-31130

【特許請求の範囲】

【請求項1】 正当な権利を有するユーザのみにサービスを提供するサービス提供装置において、
認証用データを記憶する第1の記憶手段と、
ユーザの固有情報を記憶する第2の記憶手段と、
前記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第3の記憶手段と、
前記第1の記憶手段に保持されている認証用データと、
前記第2の記憶手段に記憶されている前記ユーザの固有情報と、前記第3の記憶手段に記憶されている前記証明用補助情報とに所定の計算を施して証明データを生成する証明データ生成手段とを有し、
前記証明データ生成手段によって生成された証明データを利用してサービスを提供することを特徴とするサービス提供装置。

【請求項2】 正当な権利を有するユーザのみにサービスを提供するサービス提供装置において、
認証用データを記憶する第1の記憶手段と、
ユーザの固有情報を記憶する第2の記憶手段と、
前記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第3の記憶手段と、
前記第1の記憶手段に保持されている認証用データと、
前記第2の記憶手段に記憶されている前記ユーザの固有情報と、前記第3の記憶手段に記憶されている前記証明用補助情報とに所定の計算を施して証明データを生成する証明データ生成手段と、
前記証明データ生成手段によって生成された証明データが前記アクセス資格認証の特徴情報に基づいて生成されていることを検証する証明データ検証手段とを有し、
前記証明データ検証手段による検証が成功した場合にのみ、サービスを提供することを特徴とするサービス提供装置。

【請求項3】 利用を制限された情報を入力する入力手段を更に有し、
前記証明データ検証手段による検証が成功した場合にのみ、前記情報に対する利用の制限を解除して情報の利用を可能にすることを特徴とする請求項2に記載のサービス提供装置。

【請求項4】 前記アクセス資格認証の特徴情報が暗号化関数における復号鍵であり、前記認証用データが適当なデータを前記復号鍵に対応する暗号化鍵を用いて暗号化したものであり、
前記証明データ検証手段は、前記証明データ生成手段が生成する証明データが前記認証用データを正しく復号したものである場合に検証が成功したと判定することを特徴とする請求項2または3に記載のサービス提供装置。

【請求項5】 前記アクセス資格認証の特徴情報が暗号化関数における暗号化鍵であり、

前記証明データ検証手段は、前記証明データ生成手段が生成する証明データが前記認証用データを正しく暗号化したものである場合に検証が成功したと判定することを特徴とする請求項2または3に記載のサービス提供装置。

【請求項6】 前記アクセス資格認証の特徴情報は、デジタル署名関数における署名鍵であり、前記証明データ検証手段は、前記証明データ生成手段が生成する証明データが、前記認証用データに対して、前記署名鍵を用いて正しく生成されたデジタル署名であることが検証された場合に検証が成功したと判定することを特徴とする請求項2または3に記載のサービス提供装置。

【請求項7】 前記利用を制限された情報は、少なくとも一部が暗号化された情報であり、
前記証明データ検証手段による検証が成功した場合にのみ、前記暗号化された情報を復号して情報の利用を可能にすることを特徴とする請求項2乃至6に記載のサービス提供装置。

【請求項8】 暗号化された情報を入力する入力手段を更に有し、
前記アクセス資格認証の特徴情報が暗号化関数における第1の復号鍵であり、前記認証用データが前記暗号化された情報を復号する第2の復号鍵を前記第1の復号鍵に対応する暗号化鍵を用いて暗号化したものであり、
前記証明データ生成手段によって生成された証明データが前記第2の復号鍵であり、前記第2の復号鍵を用いて前記暗号化された情報を復号して、前記情報に対応するサービスを提供することを特徴とする請求項1または2に記載のサービス提供装置。

【請求項9】 前記暗号化関数が非対称鍵暗号化関数であり、前記アクセス資格認証の特徴情報が鍵の一方であることを特徴とする請求項4、5または8に記載のサービス提供装置。

【請求項10】 前記暗号化関数が公開鍵暗号化関数であり、前記アクセス資格認証の特徴情報が秘密鍵であることを特徴とする請求項4、5または8に記載のサービス提供装置。

【請求項11】 前記暗号化関数が対称鍵暗号化関数であり、前記アクセス資格認証の特徴情報が共通秘密鍵であることを特徴とする請求項4、5または8に記載のサービス提供装置。

【請求項12】 証明データ生成装置および証明データ検証装置を具備し、前記証明データ生成装置および前記証明データ検証装置が通信を行ってユーザのアクセス資格を認証するアクセス資格認証装置を有するサービス提供装置において、
前記証明データ生成装置は、
認証用データを記憶する第1の記憶手段と、
ユーザの固有情報を記憶する第2の記憶手段と、
前記ユーザの固有情報と、アクセス資格認証の特徴情報

(3)

特開平11-31130

とに対して、所定の計算を実行した実行結果である証明用補助情報を記憶する第3の記憶手段と、

前記第1の記憶手段に保持されている前記認証用データと、前記第2の記憶手段に保持されている前記ユーザの固有情報と、前記第3の記憶手段に保持されている前記証明用補助情報とに所定の計算を実行して証明情報を生成する証明データ生成手段とを有し、

前記証明データ検証装置は、

認証用データを記憶する第4の記憶手段と、

証明データを記憶する第5の記憶手段と、

前記証明データ生成手段によって生成された前記証明データが前記アクセス資格認証用の特徴情報に基づいて生成されていることを検証する証明データ検証手段とを有し、

前記証明データ検証装置は、前記第4の記憶手段に記憶されている前記認証用データを前記証明データ生成装置の前記第1の記憶手段に書き出し、

前記証明データ生成装置は、前記証明データ生成手段によって前記第1の記憶手段に書き込まれた前記認証用データをもとに生成した前記証明データを、前記証明データ検証装置の前記第5の記憶手段に書き出し、

前記証明データ検証装置は前記第5の記憶手段に書き込まれた前記証明データを用いてユーザのアクセス資格を認証することを特徴とするサービス提供装置。

【請求項13】 前記アクセス資格認証用の特徴情報が暗号化関数の復号鍵であり、

前記証明データ検証装置が乱数生成手段と、生成した乱数を記憶する第6の記憶手段と、認証用素データを記憶する第7の記憶手段とを備え、

前記乱数生成手段は生成した乱数を前記第6の記憶手段に書き込むと共に、前記第7の記憶手段に記憶されている前記認証用素データに前記乱数を用いた乱数効果を施した後、前記認証用データとして前記第4の記憶手段に書き込み、

前記証明データ検証手段は、前記第6の記憶手段に記憶されている前記乱数による乱数効果を、前記証明データ生成装置によって前記第5の記憶手段に書き込まれた前記証明データから除去した結果が、前記アクセス資格認証の特徴情報である復号鍵で前記第7の記憶手段に記憶されている前記認証用素データを復号したものであることを検証することを特徴とする請求項12に記載のサービス提供装置。

【請求項14】 前記アクセス資格認証用の特徴情報が暗号化関数の暗号化鍵であり、

前記証明データ検証装置が乱数生成手段を備え、前記乱数生成手段は生成した乱数を前記認証用データとして前記第4の記憶手段に書き込み、

前記証明データ検証手段は、前記証明データ生成装置によって前記第5の記憶手段に書き込まれた前記証明データが、前記乱数を復号したものであることを検証するこ

とを特徴とする請求項12に記載のサービス提供装置。

【請求項15】 前記アクセス資格認証用の特徴情報がデジタル署名関数の署名鍵であり、

前記証明データ検証装置が乱数生成手段を備え、前記乱数生成手段は生成した乱数を認証用データとして前記第4の記憶手段に書き込み、

前記証明データ検証手段は、前記証明データ生成装置によって前記第5の記憶手段に書き込まれた前記証明データが、前記乱数である認証用データに対する、前記アクセス資格認証の特徴情報である署名鍵によるデジタル署名であることを検証することを特徴とする請求項12に記載のサービス提供装置。

【請求項16】 少なくとも、前記第2の記憶手段と、前記証明データ生成手段とが、内部データおよび処理手続きを外部から観測することを困難ならしめる防御手段中に保存されていることを特徴とする請求項1乃至15に記載のサービス提供装置。

【請求項17】 少なくとも、前記第2の記憶手段と、前記証明データ生成手段とが、ICカードなどの携帯可能な小型演算装置として構成されていることを特徴とする請求項1乃至15に記載のサービス提供装置。

【請求項18】 少なくとも、前記証明データ検証手段が、内部データおよび処理手続きを外部から観測することを困難ならしめる防御手段中に保存されていることを特徴とする請求項1乃至15に記載のサービス提供装置。

【請求項19】 少なくとも、前記証明データ検証手段が、ICカードなどの携帯可能な小型演算装置として構成されていることを特徴とする請求項1乃至15に記載のサービス提供装置。

【請求項20】 前記入力手段から入力される情報は、イメージ、動画、音声、音楽などのマルチメディア情報または前記マルチメディアを暗号化したものであり、前記サービスは、前記入力された情報を再生することを特徴とする請求項1乃至19に記載のサービス提供装置。

【請求項21】 前記証明データの生成を制御する利用制御情報を記憶する第8の記憶手段をさらに有し、前記第3の記憶手段に保持されている前記証明用補助情報は、前記ユーザの固有情報と、前記アクセス資格認証の特徴情報と、前記利用制御情報とに対し、所定の計算を実行した実行結果であり、

前記証明データ生成手段は、前記第1の記憶手段に保持されている認証用データと、前記第2の記憶手段に記憶されている前記ユーザの固有情報と、前記第3の記憶手段に記憶されている前記証明用補助情報と、前記第8の記憶手段に記憶されている前記利用制御情報とに所定の計算を施して証明データを生成することを特徴とする請求項1乃至20に記載のサービス提供装置。

【発明の詳細な説明】

(4)

特開平11-31130

【0001】

【発明の属する技術分野】本発明は、正当な権利を有するユーザにのみ選択的にサービスを提供することのできるサービス提供装置およびその方法に関する。

【0002】

【従来技術】近年のネットワークの発達によって、さまざまな情報がデジタル化されネットワークを通じて流通する時代が到来している。デジタル化される情報としては、文字情報ははしめ静止画、動画、音声、プログラムなどがあり、我々はネットワーク上でこれらを組み合わせたさまざまなサービスを受けることが可能である。しかし、これらデジタル情報の大きな特徴であるコピーの容易性が、これまでネットワークでのデジタル情報の流通を阻害する要因となっていた。これは、デジタル情報をコピーするとオリジナルとまったく同じ物を生成することができるため、一旦流通したものが著作権者の意図しないところで無断で使用され、著作権者が得るべき正当な対価を回収し難いという問題に起因する。

【0003】この問題を解決するため、最近では日本アイ・ビー・エム（株）のCD-SHOWCASE（商標または製品名）のように、デジタル情報を暗号化して自由に流通させ、利用する際には代金を支払って電話回線等で復号鍵を受け取り、デジタル情報を利用するようなシステムも登場している。また、特公平6-95302号公報の「ソフトウェア管理方式」には、ソフトウェアを利用した量に応じて課金し料金を回収するシステムの例が示されている。特公平7-21276号公報の「情報利用量測定装置」では、放送によって配布された情報のすべての利用者の情報利用時間等の利用量を的確に測定することができる情報利用量測定装置について述べられている。これによると情報利用量測定装置は、暗号化された書籍情報を受信し苦積し、ユーザが書籍情報を復号し表示した時間と量を利用履歴として記録しておきそれにより料金を徴収する例が示されている。

【0004】前記のシステムを実現する方法として、さまざまな暗号技術やプログラムの実行制御技術が先行技術として知られている。

【0005】プログラム実行制御技術は、

- ①アプリケーションプログラム中に、ユーザのアクセス資格認証のためのルーチンを埋め込み、
- ②該ルーチンはアプリケーションの実行を試みているユーザが正規の認証用の鍵を保有していることを検査し、
- ③前記認証用の鍵の存在が確認された場合に限りプログラムを続行し、それ以外の場合はプログラムの実行を停止する

技術である。当技術を利用することにより、認証鍵を保有する正規のユーザのみアプリケーションの実行を可能ならしめることができる。当技術は、ソフトウェア頒布事業において実用化されており、製品としては、例えば Rainbow Technologies, Inc.

社の Sentinel Super Pro（商標）や、Aladdin Knowledge Systems Ltd. 社の HASP（商標）等がある。

【0006】以下にプログラム実行制御技術についてより詳細に説明する。

①ソフトウェアの実行を行うユーザはユーザ固有情報として認証鍵を保有する。認証鍵は暗号化のための鍵であり、ソフトウェアの利用を許可する者、例えばソフトウェアベンダーがユーザに配布する。認証鍵は複製を防ぐためにハードウェア中のメモリに厳重に封入され、郵便等の物理的手段を用いてユーザに配送される。

②ユーザ認証鍵を内蔵したハードウェアを指定された方法で所有者のパソコンまたはワークステーションに装着する。ハードウェアは例えばプリンタポート等に装着される。

③ユーザがアプリケーションプログラムを起動し、プログラムの実行が前記アクセス資格認証ルーチンに及ぶと、プログラムはユーザの認証鍵を内蔵したハードウェアと通信する。通信結果に基づいてプログラムは認証鍵を識別し、正しい認証鍵の存在が確認されると次のステップへ実行を移す。通信が失敗し認証鍵の存在が確認されない場合は、プログラムは自らを停止し以降の実行ができないようにする。

【0007】アクセス資格認証ルーチンによる認証鍵の識別は、例えば次のようなプロトコルによって行われる。

①アクセス資格認証ルーチンは適当な数を生じ鍵内蔵ハードウェアに送信する。

②鍵内蔵ハードウェアは内蔵する認証鍵を用いて送られた数を暗号化し、前記アクセス資格認証ルーチンに返信する。

③認証ルーチンは、返信された数が予め予想された数、即ちハードウェアに送信した数を正しい認証鍵で暗号化して得られる数であるかを判定する。

④返信された数が予想された数と一致する場合にはプログラムの実行を継続し、一致しない場合にはプログラムを停止する。

【0008】この際のアプリケーションプログラムと認証鍵内蔵ハードウェア間の通信は、たとえ同じアプリケーションプログラム中の同じ箇所において同じハードウェアとの間で交換されるものであろうとも、実行のたびに異ならなければならない。さもなければ、正常な実行過程における通信内容を一度記録し、以後プログラムを実行するたびに記録した通信内容をアプリケーションプログラムに返信することにより、正しい認証鍵を保有しないユーザでもプログラムを実行することが可能となってしまう。このような攻撃をリプレイアタックと呼ぶ。

【0009】リプレイアタックを防ぐために、通常鍵内蔵ハードウェアに送られる数は通信のたびに新たに生成される乱数を用いる。

(5)

特開平11-31130

【0010】〔従来技術の問題点〕従来技術の問題点は、アプリケーションプログラムを作成する際に、プログラム作成者がユーザが持つ認証鍵を予め想定した上で、該認証鍵に基づいてプログラムの保護処理を行わなければならないという性質に由来する。

【0011】つまり、プログラムの作成者は、装置内蔵ハードウェアからの正しい返信をプログラム作成時に予測して、正しい返信を受けた場合にのみプログラムが正常に実行されるようにプログラムの作成を行わなければならない。

【0012】前記の特徴を有する従来技術の利用形態は基本的に前記の二通りとなるが、いずれの場合も以下に述べる問題を有する。

【0013】①第1の方法では、ユーザの認証鍵をユーザ毎に異なるように用意する。即ち、ユーザ甲には認証鍵甲、ユーザ乙には認証鍵乙というように、ユーザごとに異なる認証鍵を1つずつ用意する。この場合、プログラム中の認証ルーチンは該プログラムを利用するユーザの固有の認証鍵を認証できるように作成されなければならない、プログラム作成者は利用ユーザの数だけ異なるプログラムを作成する必要がある。

【0014】対象となるユーザが多数の場合、プログラムをユーザ毎にカスタマイズ（個別化）する作業はプログラム作成者にとって耐え難い労力を要求し、管理しなければならないユーザ認証鍵のリストも膨大なものとなる。

【0015】②第2の方法では、プログラムの作成者はアプリケーションごとにそれぞれ異なる認証鍵を用意する。即ち、アプリケーション甲には認証鍵甲、アプリケーション乙には認証鍵乙というように、アプリケーションごとに異なる認証鍵を1つずつ用意し、固有の認証鍵を識別するように各アプリケーションプログラムを作成する。

【0016】この方法では、第1の方法のようにユーザ毎にプログラムを個別的に作成する必要はなくなるが、逆にユーザは利用するアプリケーションの数だけ認証鍵を保持しなければならないことになる。

【0017】上述のように、認証鍵はハードウェアに厳重に封入した状態でユーザに配布する必要がある。従って、プログラム自身はネットワークを介して簡便に配布することができるのに対し、認証鍵を内蔵するハードウェアの配布は郵便等の物理的手段に頼らざるを得ない。プログラム作成者はユーザからのアプリケーションの使用許諾以来を上げ取るたびに、そのアプリケーションに対応する認証鍵が封入されたハードウェアを郵送する必要がある、コスト、時間、梱包の手間いずれをとってもプログラム作成者にとって大きな負担となる。

【0018】また、ユーザは利用するアプリケーションを変更するたびにハードウェアを交換しなければならないという煩雑さに甘んじなければならない。

【0019】ユーザがあるアプリケーションを使いたいとしても、認証鍵が封入されたハードウェアが郵送されて到着するまで待たなければならない、即座に利用できないという問題もある。

【0020】これら問題を軽減するために、ハードウェア中に予め複数の認証鍵を封入しておき、新しいアプリケーションの利用をユーザに許可するたびに、ハードウェア中の認証鍵を利用可能とするためのパスワードをユーザに教えるという方法を用いることはできるが、予め封入された認証鍵を使い切った場合は同様の問題が発生し、本質的な解決とはなっていない。

【0021】前記のような実効制御の方法以外に、単にアプリケーションを暗号化して、その復号鍵を安全な方法でユーザに教えるという単純な方法が一般的に広く用いられているが、この方法では、アプリケーションを一旦復号してしまうと、ユーザは好きなようにアプリケーションをコピーして不正に配ることができると、ほとんど防衛されていないとみなしてよい。

【0022】従って、デジタル化された情報、例えばソフトウェア、音楽、映画等（以後これらを総称してコンテンツと呼ぶ）をネットワークで配送して、正当な対価を得ようとした場合、従来の技術では、コンテンツの管理が煩雑になったり、認証用のハードウェアの管理でユーザに大きな負担をかけてしまうという問題があった。

【0023】

【発明が解決しようとする課題】本発明は、このような問題に鑑みなされたものであり、ユーザおよびサービス提供者の負担を最小限に押さえながら、サービスの利用を正当な権利を有するユーザにのみ提供することができるシステム、または、サービスの利用に応じた正当な対価を回収することが可能なシステムを提供することを目的とする。

【0024】

【課題を解決するための手段】本発明の第1の側面によれば、上述の目的を達成するために、正当な権利を有するユーザのみにサービスを提供するサービス提供装置に、認証用データを記憶する第1の記憶手段と、ユーザの固有情報を記憶する第2の記憶手段と、前記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第3の記憶手段と、前記第1の記憶手段に保持されている認証用データと、前記第2の記憶手段に記憶されている前記ユーザの固有情報と、前記第3の記憶手段に記憶されている前記証明用補助情報とに所定の計算を施して証明データを生成する証明データ生成手段とを設けるようにしている。

【0025】また、本発明の第2の側面によれば、正当な権利を有するユーザのみにサービスを提供するサービス提供装置に、認証用データを記憶する第1の記憶手段と、ユーザの固有情報を記憶する第2の記憶手段と、前

(6)

特開平11-31130

記ユーザの固有情報と、アクセス資格認証の特徴情報とに対し、所定の計算を実行した実行結果である証明用補助情報を記憶する第3の記憶手段と、前記第1の記憶手段に保持されている認証用データと、前記第2の記憶手段に記憶されている前記ユーザの固有情報と、前記第3の記憶手段に記憶されている前記証明用補助情報とに所定の計算を施して証明データを生成する証明データ生成手段と、前記証明データ生成手段によって生成された証明データが前記アクセス資格認証の特徴情報に基づいて生成されていることを検証する証明データ検証手段とを設けるようにしている。

【0026】これらの構成によれば、証明用補助データ（アクセスチケット）を導入することにより、プロテクト側で付与されるアクセス資格認証の特徴情報とユーザ側に付与されるユーザ固有情報とを独立させることができ、ユーザは予めユーザ固有情報を所持し、プログラム作成者等のプロテクト者はユーザが所持するユーザ固有情報とは独立にアクセス資格認証の特徴情報を用いてアプリケーションプログラムを作成し、その後、アクセスチケットをユーザの固有情報とアプリケーションプログラムの作成等に使用したアクセスチケット資格認証の特徴情報とに応じて作成し、配布することにより、実行制御等のユーザアクセス資格の認証を行うことが可能となり、正当な権利を有するユーザにのみ所望のサービスを提供することができる。また、証明データ生成時にログを取るようによれば、サービスに対する正当な対価を回収することができる。

【0027】また、前記の構成においては、少なくとも前記第2の記憶手段と、前記証明データ生成手段とが、内部データおよび処理手続きを外部から観測することが困難ならしめる防御手段中に保持されるようにしてもよい。

【0028】また、前記の構成においては、少なくとも前記証明データ検証手段が、内部データおよび処理手続きを外部から観測することが困難ならしめる防御手段中に保持されるようにしてもよい。

【0029】また、前記アクセス資格認証の特徴情報が暗号化関数における復号鍵であり、前記認証用データが適当なデータを前記復号鍵に対応する暗号化鍵を用いて暗号化したものであり、前記証明データ検証手段により、前記証明データ生成手段が生成する証明データが前記認証用データを正しく復号したものであることを検証するようにしてもよい。また、前記アクセス資格認証の特徴情報が暗号化関数における暗号化鍵であり、前記認証用データが適当なデータを前記暗号化鍵に対応する復号鍵を用いて復号したものであり、前記証明データ検証手段により、前記証明データ生成手段が生成する証明データが前記認証用データを正しく暗号化したものであることを検証するようにしてもよい。また、前記アクセス資格認証の特徴情報がデジタル署名関数における署名鍵

であり、前記証明データ生成手段が生成する証明データが、前記認証用データに対して、前記署名鍵を用いて正しく生成されたデジタル署名であることを検証するようにしてもよい。

【0030】また、前記アクセス資格認証の特徴情報が暗号化関数における第1の復号鍵であり、前記認証用データが前記暗号化された情報を復号する第2の復号鍵を前記第1の復号鍵に対応する暗号化鍵を用いて暗号化したものであり、前記証明データ生成手段によって生成された証明データが前記第2の復号鍵であり、前記第2の復号鍵を用いて前記暗号化された情報を復号して、前記情報に対応するサービスを提供するようにしてもよい。また、前記暗号化関数が非対称鍵暗号化関数であり、アクセス資格認証の特徴情報が鍵の一方であってもよい。

【0031】また、前記暗号化関数が公開鍵暗号化関数であり、アクセス資格認証の特徴情報が秘密鍵であってもよい。

【0032】また、前記暗号化関数が対称鍵暗号化関数であり、アクセス資格認証の特徴情報が共通秘密鍵であってもよい。

【0033】また、前記第1の記憶手段と、前記第2の記憶手段と、前記第3の記憶手段と、前記証明データ生成手段とから構成される証明データ生成装置と、前記証明データ検証手段に加え、認証用データを記憶する第4の記憶手段と、証明データを記憶する第5の記憶手段をそなえた証明データ検証装置とが、互いに通信することによりユーザのアクセス資格を認証するアクセス資格認証装置を有するサービス提供装置において、証明データ検証装置は、第4の記憶手段に記憶されている認証用データを証明データ生成装置の第1の記憶手段に書き出し、証明データ生成装置は、証明データ生成手段によって第1の記憶手段に書き込まれた前記認証用データをもとに生成した証明データを、証明データ検証装置中の第5の記憶手段にかき出し、証明データ検証装置は第5の記憶手段に書き込まれた前記証明データを用いてユーザのアクセス資格を認証するようにすることもできる。

【0034】また、アクセス資格認証の特徴情報が暗号化関数の復号鍵であり、証明データ検証装置が乱数生成手段と、生成した乱数を記憶する第6の記憶手段と、認証用素データを記憶する第7の記憶手段とを備え、乱数生成手段は生成した乱数を第6の記憶手段に書き込むと共に、第7の記憶手段に記憶されている認証用素データに前記乱数を用いた乱数効果を施した後、認証用データとして第4の記憶手段に書き込み、証明データ検証手段は、第6の記憶手段に記憶されている乱数による乱数効果を、前記証明データ生成装置によって第5の記憶手段に書き込まれた証明データから除去した結果が、アクセス資格認証の特徴情報である復号鍵で第7の記憶手段に記憶されている認証用素データを復号したものであることを検証するようにしてもよい。

(7)

特開平11-31130

【0035】また、アクセス資格認証用の特徴情報が暗号化関数の暗号化鍵であり、証明データ検証装置が乱数生成手段を備え、乱数生成手段は生成した乱数を認証用データとして第4の記憶手段に書き込み、証明データ検証手段は、証明データ生成装置によって第5の記憶手段に書き込まれた証明データが、前記乱数を復号したものであることを検証するようにしてもよい。

【0036】また、アクセス資格認証用の特徴情報がデジタル署名関数の署名鍵であり、証明データ検証装置が乱数生成手段を備え、乱数生成手段は生成した乱数を認証用データとして第4の記憶手段に書き込み、証明データ検証手段は、証明データ生成装置によって第5の記憶手段に書き込まれた証明データが、前記乱数である認証用データに対する、アクセス資格認証の特徴情報である署名鍵によるデジタル署名であることを検証するようにしてもよい。

【0037】

【発明の実施の態様】以下、この発明を詳細に説明する。

【実施例1】まず、実施例1を参照して本発明の原理的な構成について説明する。図1は本発明の実施例1の構成を全体として示すものであり、この図1においてサービス提供システムは、証明データ検証装置10および証明データ生成装置11からなっており、証明データ生成装置11はアクセスチケット生成装置12からアクセスチケット（証明用補助データ）13を受領するようになっている。証明データ検証装置10は検証ルーチン15を実行する。証明データ生成装置11はユーザ固有情報16およびアクセスチケット13を保持し、証明データ生成プログラム17を実行する。ユーザ固有情報16および証明データ生成プログラム17の少なくとも一部が耐タンパー装置20で保護されている。

【0038】アクセスチケット生成装置12はアクセス資格認証の特徴情報14およびユーザの固有情報16に基づいてアクセスチケット13を生成し、アクセスチケット13はネットワークや記憶媒体等を通してユーザに送られ、ユーザの証明データ生成装置11に保持される。

【0039】証明データ検証装置10は認証用データ18を証明データ生成装置11に送信する。証明データ生成装置11はアクセスチケット13およびユーザ固有情報16を用いて証明データ19を生成し、これを証明データ検証装置10に返信する。証明データ検証装置10は認証用データに基づいて証明データの正当性を検証する。即ち、証明データが、検証用データとアクセス資格認証の特徴情報とに基づいて生成されたデータであることを検証する。

【0040】証明データの正当性が検証されれば、ユーザが正当な権利を有することが認証され、サービス提供装置により所望のサービスが提供される。

【0041】以下、図2を用い、実際のサービスを例にとって本発明を具体的に説明する。

【0042】本発明の実施例1では、インターネットブラウザ（Netscape Navigator—米国ネットスケープ・コミュニケーションズ社の商標—等）に、証明データ検証ルーチン15と復号プログラム35とを一体化してプラグイン（Plug-in）モジュールとして組み込んだ例について述べる。ここで、プラグイン・モジュールとはインターネットブラウザの機能を拡張するソフトウェアプログラムを指し、これにより、ユーザに新しいデータタイプの利用をサポートすることができる。インターネットブラウザがサポートしていないデータタイプの情報をサーバから受け取ると、インターネットブラウザは、そのデータタイプに関連付けられているプラグインを探してロードし、起動する。これにより、ユーザの既存のシステムを変更することなく、シームレスに新しいデータタイプのサポートを可能にするものである。

【0043】本実施例の場合の新しいデータタイプとは暗号化されたコンテンツ34を指し、インターネットブラウザが暗号化されたコンテンツ34をサーバから受け取ると、インターネットブラウザは暗号化されたコンテンツ34のデータタイプを見て、そのデータタイプに関連付けられているプラグイン38を探してロードし、起動する。起動されたプラグインは、検証ルーチン15を起動し、証明用プログラム32に認証用データを送り、返ってきた証明データを用いて検証を行う。検証ルーチン15により検証が成功した場合には復号プログラム35によって、暗号化されたコンテンツ34が復号されてユーザに提供される。復号されたコンテンツは、ハイパーテキストドキュメント、画像、動画、音楽などの情報やダウンロードしたプログラムなどである。

【0044】証明データ生成装置は、証明用プログラム32とトークン33とで構成される。認証用プログラム32はアクセスチケット13と認証データ生成プログラムA36を含むソフトウェアプログラムであり、ユーザのパーソナルコンピュータ（PC）上で動作する。トークン33は認証データ生成プログラムB37とユーザ固有情報16とを含み、プロープによる内部状態の窃盗への防御力を有するハードウェア（以下、耐タンパーハードウェアと呼ぶ）により構成することが望ましい。なぜならば、ユーザ固有情報は、パスワード認証におけるパスワードに相当するものであり、ユーザの身許を証明する唯一の重要な情報であり、ユーザ固有情報16を読み出しコピーして配布することができると、正当な権利を持たない者にコンテンツの不正利用を許してしまうことになる。

【0045】また、ユーザには前記ユーザ固有情報に加え、所定の計算手続きを実行する証明データ生成プログラムA、Bが与えられる。このプログラムは、プラグイ

(8)

特開平11-31130

ン38中の検証ルーチン15と通信を行うためのものであり、ユーザ固有情報16とアクセスチケット13が与えられると、認証用データ42に対して計算を行いユーザの身許を証明する証明データ45を生成する。この計算の過程でユーザ固有情報16が用いられるが、上述した理由によりユーザ固有情報16が外部に漏洩すると問題があるため、ユーザ固有情報を用いる証明データ生成プログラムB37は前記耐タンパハードウェア内に収められる。耐タンパハードウェアとしては、ICカードや樹脂モールド等で保護されたICチップなどが簡便で適用しやすい。しかし、提供するサービスの付加価値が非常に高い場合は、特願平08-284475号の「暗号化装置、復号装置、機密データ処理装置、および情報処理装置」で示されるような、高い安全性を有する装置を用いてもよい。

【0046】証明データ検証ルーチン15の作用を以下に数例述べる。

【0047】1. 証明データ検証ルーチン15中には、送信すべきデータ（認証用データ42）と期待される返信データ（期待値）が埋入されている。証明データ検証ルーチン15は、前記送信データを取り出してユーザに送信し、ユーザから返信を受け取る。次いで、ユーザからの返信データと前記期待値とを比較して、両者が一致した場合に復号プログラム35により暗号化されたコンテンツ34を復号して、ユーザに利用可能な状態でコンテンツを提供する。

【0048】2. 証明データ検証ルーチン15中には、送信すべきデータと期待される返信データ（期待値）が埋入されている。証明データ検証ルーチン15は、前記送信データを取り出してユーザに送信し、ユーザから返信を受け取る。次いで、ユーザからの返信データに一方方向関数を施した値を、前記期待値と比較して、両者が一致した場合に復号プログラム35により暗号化されたコンテンツ34を復号して、ユーザに利用可能な状態でコンテンツを提供する。

【0049】上記1、2の作用において、返信データが送信データの所定の暗号化アルゴリズムに従う暗号化の結果であるとした場合には、アクセス資格認証の特徴情報は暗号化鍵となる。また、返信データが送信データの所定の署名アルゴリズムに従うデジタル署名であるとした場合には、アクセス資格認証の特徴情報は署名鍵となる。

【0050】3. 証明データ検証ルーチン15中には、送信すべきデータが埋入されている。証明データ検証ルーチン15は、前記送信データを取り出してユーザに送信し、ユーザから返信を受け取る。次いで、前記返信データを復号鍵として、復号プログラム35により暗号化されたコンテンツ34を復号して、ユーザに利用可能な状態でコンテンツを提供する。

【0051】4. 証明データ検証ルーチン15中には、

送信すべきデータが埋入されている。証明データ検証ルーチン15は、前記送信データを取り出して乱数効果を付与した後ユーザに送信し、ユーザから返信を受け取る。次いで、前記返信データから前記乱数効果を取り除いた結果を復号鍵として、復号プログラム35により暗号化されたコンテンツ34を復号して、ユーザに利用可能な状態でコンテンツを提供する。

【0052】5. 証明データ検証ルーチン15は、暗号化されたコンテンツに対応した送信データを受け取る。この場合、送信データは暗号化されたコンテンツの中に埋入されていてもよい。証明データ検証ルーチン15は、受け取った前記送信データをユーザに送信し、ユーザから返信を受け取る。次いで、前記返信データを復号鍵として、復号プログラム35により暗号化されたコンテンツ34を復号して、ユーザに利用可能な状態でコンテンツを提供する。

【0053】6. 証明データ検証ルーチン15は、暗号化されたコンテンツに対応した送信データを受け取る。この場合、送信データは暗号化されたコンテンツの中に埋入されていてもよい。証明データ検証ルーチン15は、受け取った前記送信データに乱数効果を付与した後ユーザに送信し、ユーザから返信を受け取る。次いで、前記返信データから前記乱数効果を取り除いた結果を復号鍵として、復号プログラム35により暗号化されたコンテンツ34を復号して、ユーザに利用可能な状態でコンテンツを提供する。

【0054】上記3乃至6の作用において、返信データから正しい復号鍵が得られた場合にかぎって、暗号化されたコンテンツ34は正しく復号され、ユーザは該コンテンツを利用可能となる。この場合のアクセス資格認証の特徴情報は暗号化された復号鍵を復号するための復号鍵となる。

【0055】さて、従来の例で述べた実行制御技術では、ユーザ固有情報（ユーザの認証鍵）がアクセス資格認証の特徴情報と同一のものである。従来の証明データ生成ルーチンはアクセス資格認証の特徴情報と証明データ検証ルーチンから送信されたデータとを入力して、返信データを計算する。

【0056】これに対し本発明の特徴は、ユーザ固有情報16とアクセス資格認証の特徴情報14とが互いに独立である点にある。この構成でも、証明データ生成プログラムAとBはユーザ固有情報16と証明データ検証ルーチン15から送信されたデータ42に加えて、アクセスチケット13を入力として返信データ（証明データ）45を計算する。この構成は以下の性質を持つ。

【0057】1. アクセスチケット13は特定のユーザ固有情報16とアクセス資格認証の特徴情報14とに基づいて計算されるデータである。

2. ユーザ固有情報16を知らずにアクセスチケット13から、アクセス資格認証の特徴情報14を計算するこ

(9)

特開平11-31130

とは少なくとも計算量的に不可能である。

3. 証明データ生成プログラムAとBは、ユーザ固有情報16とアクセスチケット13とが正しい組み合わせの場合、即ち、ユーザ固有情報16とアクセスチケット13との正しい組み合わせが入力された場合に限って、正しい返信データを計算する。

【0058】以上により、ユーザはあらかじめユーザ固有情報16を所持し、コンテンツ作成者はユーザが所持するユーザ固有情報16とは独立にコンテンツを暗号化し、アクセスチケット13をユーザ固有情報16とアクセス資格認証の特徴情報とに応じて作成することで、正当な権利を有するユーザにのみユーザ固有情報16とは独立に暗号化されたコンテンツの利用を享受することができる。

【0059】また、ユーザ固有情報16を二つの固有情報からなるものとし、アクセスチケット13の作成に際して用いる固有情報と、ユーザが通信プログラムにおいて用いる固有情報とを区別して用いることもできる。最も典型的な例は、ユーザ固有情報16を公開鍵ペアとし、公開鍵を公開固有情報としてアクセスチケット作成に用い、秘密鍵をユーザ個人の秘密固有情報としてトークン33内に封入しておく方法である。この場合はアクセスチケット13をアクセス資格認証の特徴情報14と前記公開鍵ペアの公開鍵から計算できるようにすることにより、秘密鍵であるユーザ固有情報16を秘密に保ったままアクセスチケット13を計算することが可能となる。

【0060】次により具体的な構成について実施例に照して説明する。図2において、インターネットブラウザ31とプラグイン38と証明用プログラム32は、ユーザの用いる計算機30（PCあるいはワークステーション）上のソフトウェアプログラムとして実現することができる。トークン33についても同様にソフトウェアプログラムとして実現してもよいが、ユーザを識別するための固有情報（ユーザ固有情報）の安全性を高めるために、該計算機30に接続される耐タンパ特性を有するトークン33（ICカード、PCカード、ボード等）を併用するのが望ましい。この際、ICカードのような携帯性を有するハードウェアを用いれば、ユーザが複数のPCあるいはワークステーション上で作業する場合に便利である。

【0061】インターネットブラウザ31で利用する暗号化されたコンテンツ34は、ネットワークやCD-ROM、DVD、フロッピーディスク等の記憶媒体を用いてユーザに供給される。

【0062】ユーザがインターネットブラウザから暗号化されたコンテンツの利用を要求すると、インターネットブラウザは暗号化されたコンテンツのデータタイプを見て、そのデータタイプに関連付けられているプラグインを探してロードし、起動する。

【0063】プラグインが起動すると、該プラグイン中の検証プログラムが起動し、証明用プログラム32と通信してユーザ認証を行い、通信が正しく終了した場合に限って、該コンテンツの復号を実行する。

【0064】ユーザが暗号化されたコンテンツ34を利用するためには、ユーザ本人宛に発行されたアクセスチケット（証明用補助情報）を取得する必要がある。ユーザは前記PCあるいはワークステーション上にインストールされた証明用プログラム32に、取得したアクセスチケットを登録するとともに、例えばユーザ固有情報がICカードに封入されている場合には、ICカードを前記PCあるいはワークステーションに装着する。

【0065】証明データ生成プログラムAは、証明データ生成プログラムBと協調して、ユーザ固有情報16とアクセスチケット13とに基づいて計算を行い、その計算に基づいてプラグイン中の検証プログラム15と通信を行う。

【0066】通信の結果、検証プログラム15による認証が成功するのは、ユーザ固有情報と、アクセスチケットと、暗号化されたコンテンツとの3つが正しく対応している場合に限る。ユーザ固有情報あるいはアクセスチケットの一方が欠けていた場合には認証は成功しない。

【0067】アクセスチケットは特定のユーザ宛に発行される。即ち、アクセスチケットの生成に際して、特定のユーザのユーザ固有情報が使用される。アクセスチケット生成時に使用されるユーザ固有情報と、証明データ生成プログラムによって使用される前記ユーザ固有情報とが一致していない場合、やはり、認証は成功しない。

【0068】また、アクセスチケットは、特定のアクセス資格認証の特徴情報に基づいて生成され、検証プログラム15はこのアクセス資格認証の特徴情報を認証するように構成される。従って、アクセスチケットの生成のもととなった特徴情報と、検証プログラム15が認証しようとする特徴情報とが互に対応していなかった場合にも、認証は成功しない。

【0069】アクセスチケットは、それ自身十分な安全性を備えていることから、ネットワークを介して配送することができる。アクセスチケットの安全性とは、以下の二つの性質である。

【0070】1. アクセスチケットは記名式であり、アクセスチケットが発行されたユーザ本人（正確には、アクセスチケット生成時に用いられたユーザ固有情報の保持者）だけが該アクセスチケットを用いて証明データ生成装置を正しく作動させることができる。従って、悪意の第三者がネットワークを盗聴し、他のユーザのアクセスチケットを不正に手に入れたとしても、この第三者がアクセスチケットの発行先である正規のユーザ固有情報を手に入れない限り、このアクセスチケットを利用することは不可能である。

【0071】2. アクセスチケットはさらに厳密な安全

(10)

特開平11-31130

性を保持している。即ち、悪意の第三者が任意の個数のアクセスチケットを集めて、いかなる解析を行ったとしても、得られた情報をもとに別のアクセスチケットを偽造したり、証明データ生成装置の動作を模倣して認証を成立させるような装置を構成することは不可能である。

【0072】実施例1では、アクセスチケット t は次の式1に基づいて生成されるデータである。

【0073】

【数1】

$$(1) \quad t = D - e + \omega \phi(n)$$

上式中の記号はすべて整数であり、以下を表す。 n はRSA (Rivest-Shamir-Adelman) 法数、即ち十分大きな二つの素数 p 、 q の積である($n = pq$)。 $\phi(n)$ は n のオイラー数、即ち、 $p-1$ と $q-1$ の積である($\phi(n) = (p-1)(q-1)$)。 e はユーザ固有情報を表し、ユーザ毎に異なる数で、ユーザを識別するために用いる。 D はアクセスチケット秘密鍵すなわちアクセス資格認証の特徴情報を表し、法数 n のもとでのRSA秘密鍵であり、式2を満たす。

【0074】

$$\text{【数2】} (2) \quad \gcd(D, \phi(n)) = 1$$

ここで、 $\gcd(x, y)$ は二数 x 、 y の最大公約数を表す。式(2)によって表現される性質は、式3を満たす数 E が存在することを保証する。

【0075】

$$\text{【数3】} (3) \quad ED \bmod \phi(n) = 1$$

E をアクセスチケット公開鍵と呼ぶ。

【0076】 ω は、 n および e に依存して定まる数であり、 n あるいは e のいずれか一方が異なる場合、その値が容易に一致しない(衝突しない)ように定める。 ω の定め方の一例として、一方向性ハッシュ関数 h を利用して、式4のように ω を定める方法もある。

【0077】

$$\text{【数4】} (4) \quad \omega = h(n|e)$$

ただし、記号 $|$ はビット列の結合を表す。

【0078】一方向性ハッシュ関数とは、 $h(x) = h(y)$ を満たす相異なる x 、 y を算出することが著しく困難であるという性質を持つ関数である。一方向性ハッシュ関数の例として、RSA Data Security Inc. によるMD2、MD4、MD5、および米国連邦政府による規格SHS (Secure Hash Standard) が知られている。

【0079】上記の説明中に現れた数において、 t 、 E および n は公開可能であり、残りの D 、 e 、 ω 、 p 、 q および $\phi(n)$ はチケットを作成する権利を有する者以外には秘密である必要がある。

【0080】図3に、ユーザが用いる計算機(PCあるいはワークステーション)の概略図を示す。図3においては、ユーザが用いる計算機30に、カードリーダー39

が接続されており、ユーザはカードリーダー39にトークン33を挿入して利用する。インターネットブラウザ31、プラグイン、証明用プログラムは、計算機30上のソフトウェアプログラムとして実現されている。また、アクセスチケットも計算機30の記憶領域に記憶されている。今、利用しようとしているコンテンツは、ヨットの絵の画像であり、正当なトークンと正当なアクセスチケットを持つユーザが、暗号化されたコンテンツをインターネットブラウザ31に読み込ませると、図3に示すようにプラグインによってインターネットブラウザ31上に、ヨットの絵の画像が表示される。

【0081】図4を参照してさらに実施例1について詳細に説明する。図4は、本発明の実施例1の構成例を具体的に示すものである。図2と対比させると検証ルーチン15に対応するものは、アクセスチケット公開鍵記憶部51、認証データ記憶部52、乱数発生部53、乱数記憶部54、送信データ(チャレンジ)計算部55、データ分離部56、証明データ受信部57、乱数効果除去部58、および検証部59とで構成され、復号プログラム35は、復号/表示部61に対応する。この例では検証ルーチンと復号プログラムとを分けて構成してあるが、必要に応じて復号プログラムを検証ルーチンに併合させてもよい。また、証明用プログラム32は、認証用データ受信部71、アクセスチケット記憶部72、第1演算部73および証明データ生成部76とで構成され、トークン33はユーザ固有情報記憶部74および第2演算部75とで構成される。

【0082】次に、動作について説明する。以下の説明における変数は、すべて整数である。

【0083】[ステップ1]: ユーザがインターネットブラウザから暗号化されたコンテンツの利用を要求すると、インターネットブラウザは暗号化されたコンテンツのデータタイプを見て、そのデータタイプに関連付けられているプラグインを探してロードし、起動する。対応するプラグインが起動すると、プラグイン中の検証ルーチン15が立ち上がる。この場合のコンテンツとはユーザがインターネットブラウザを通して利用するようなものを指し、例えばホームページの表示情報(画像、動画、ハイパードキュメントなど)であったり、Java アプレットのようなプログラムであったりする。

【0084】[ステップ2]: プラグインの検証ルーチン15は、データ分離部において暗号化されたコンテンツからアクセスチケット公開鍵(E 、 n)と認証データ KE を取り出し、それぞれアクセスチケット公開鍵記憶部51と認証データ記憶部52に格納する。ここでは、該アクセスチケット公開鍵と該認証データは、暗号化されたコンテンツに付随して配布されているものとして説明した。このように該アクセスチケット公開鍵と該認証データは、暗号化されたコンテンツに付随していてもよいしネットワークを通して入手できるようにしてもよい

動作

(11)

特開平11-31130

が、安全性を考えると暗号化されたコンテンツに付随しているのが望ましく、さらに、該認証データは、ユーザにはわからないように埋め込まれていることが望ましい。例えば、該認証データは、暗号化してコンテンツの中に埋め込んでおき、取り出したあと、プラグインに持たせた復号鍵で復号するなどの方法を取ればよい。

【0085】【ステップ3】：次に、検証ルーチン15は、乱数生成部63で乱数 r を生成し乱数記憶部54に格納し、アクセスチケット公開鍵 (E, n) と認証データ KE および乱数 r を用いて送信データ（チャレンジ） C を式5に従って計算する。

【0086】

【数5】(5) $C = rEK_E \bmod n$

チャレンジ C とアクセスチケット公開鍵法数（RSA法数） n は、証明データ生成側に送信される。 C の値には乱数 r が含まれているため、通信の度に異なる値となり、リプレイアタックを防止する効果を持つ。

【0087】【ステップ4】：証明用プログラムでは、検証ルーチンから送られたチャレンジ C とRSA法数 n とを認証用データ受信部で受信し、証明データ（レスポンス） R を以下のようにして生成する。まず、第1演算部ではアクセスチケット記憶部72から、RSA法数 n をキーにして対応するアクセスチケット t を取得し、RSA法数 n のもとで、式6を実行し中間情報 R' を得る。

【0088】

【数6】(6) $R' = Ct \bmod n$

【ステップ5】：第2演算部75は、ユーザ固有情報記憶部74に記憶されているユーザ固有情報 e を取得し、式7を実行し差分情報 S を得る。

【0089】

【数7】(7) $S = Ce \bmod n$

【ステップ6】：そして、証明データ生成部76は第1および第2演算部73、75から中間情報 R' および差分情報 S を得て、式8の計算を行い証明データ R を得る。

【0090】

【数8】(8) $R = R' S \bmod n$

証明データ R は、検証ルーチンに送信される。

【0091】【ステップ7】：検証ルーチン15の乱数効果除去部58は、証明データ受信部67で受信した証明データ R を取得し、乱数記憶部54に記憶されている乱数 r とにより、式9の計算を行い K' を得る。

【0092】

【数9】(9) $K' = Rr^{-1} \bmod n$

【ステップ8】：検証部59では、前記乱数効果除去部58で計算した K' がアクセス資格認証の特徴情報である D に基づいて生成されていることを検証する。 K' が正しくアクセス資格認証の特徴情報である D に基づいて生成されている場合には、 $K' = K$ が成り立つはずであ

る。この式が成り立つかどうかは、この K' を用いて暗号化されたデータを復号してみて、正しく復号されるかどうかを判定する方法や、 K に冗長性をもたせ、その部分に特定の値を持たせておき、 K' がその特定の値を持っているかどうかで判定する方法などがある。後者の方法には、国際規格ISO9796などの方法を用いることができる。ここでは、後者の方法を用いて、検証することを前提に説明を続ける。

【0093】【ステップ9】：検証部59での検証が正しいと判定されると、検証ルーチンは復号／表示部61へ復号鍵 K' を渡す。

【0094】【ステップ10】：復号／表示部61は、検証部59から復号鍵 K' を受け取り、データ分離部56で分離した暗号化されたコンテンツを復号して表示する。復号されたコンテンツをインターネットブラウザへ渡して、インターネットブラウザで表示する方法も可能であるが、復号された情報がインターネットブラウザによりコピーされる可能性があるため、安全性の面からは、インターネットブラウザが指定した領域にプラグインが直接表示するほうが望ましい。

【0095】このようにして、正当な権利を有するユーザはインターネットブラウザを用いて暗号化されたコンテンツを利用することができる。このとき、復号されたコンテンツは一時的にしかメモリ上に存在せず、ユーザの利用が終わると消滅するようにすることで、復号されたコンテンツの不正利用を防ぐことができる。

【0096】本実施例では、暗号化されたコンテンツは、アクセスチケット公開鍵 (E, n) と認証データ KE とを付随して配布されるものとして説明した。この暗号化されたコンテンツの構成例を図5に示す。図5に示すように、暗号化されたコンテンツは、アクセスチケット公開鍵 (E, n) と、認証データ KE と、暗号化されたコンテンツ本体とから構成される。検証ルーチンのデータ分離部は、これらを読み込んで、各部分に分離する。

【0097】コンテンツ本体は鍵 K で暗号化されており、認証データ KE を用いて正しく検証が終了すると、乱数効果除去部を通して鍵 K を復元することができ、この鍵 K を用いてコンテンツ本体を復号することが可能になる。

【0098】安全性をより高めるためには、認証データ KE がユーザには容易に分離できないように埋め込まれていることが望ましい。この実現の一方方法を、図6に示す。図6では、図5と同様に、暗号化されたコンテンツは、アクセスチケット公開鍵 (E, n) と認証データ KE と暗号化されたコンテンツ本体とから構成されるが、コンテンツ本体だけでなく、認証データ KE もさらに暗号化されている。図6では、認証データ KE は鍵 K_p により暗号化されているものとして示した。

【0099】検証ルーチンのデータ分離部は、この暗号

(Fig. 4)
→ 1
↑

(12)

特開平11-31130

鍵 K_p に対応する復号鍵 K_p を保持しており（共通鍵暗号を用いる例）、入力されたコンテンツ全体から、アクセスチケット公開鍵（ E, n ）と、暗号化された認証データ KE と、暗号化されたコンテンツ本体とを分離し、保持している復号鍵 K_p を用いて暗号化された認証データを復号して、認証データ KE を取り出す。その後、この認証データ KE を用いて検証を行い、正しく検証が終了すると、乱数効果除去部を通して鍵 K を復元することができ、この鍵 K を用いてコンテンツ本体を復号することが可能になる。

【0100】ここでは、コンテンツ本体や認証データを暗号化するのに、共通鍵暗号方式を用いた例を示したため、鍵 K や鍵 K_p は暗号化と復号化とで同じ鍵を用いる例として示したが、この部分をRSAなどの公開鍵暗号方式を用いることも可能である。

【0101】また、コンテンツの最も単純な構成例を図7に示す。この例では、コンテンツはコンテンツ本体のみから構成されており、コンテンツ本体も暗号化などの処理が行われていない。しかし、このコンテンツを利用してサービスを提供できるのは特定のプラグインだけであるという状況にある。プラグイン中の検証ルーチンでは、前述したのと同様な処理を行い、検証部における判定の結果、正当であると判断された場合にのみ、プラグインはこのコンテンツを用いてサービスを提供する。

【0102】以下では、実施例1において説明した検証ルーチンの検証部における処理の構成例を図8～図11を用いて数例述べる。図8～図11では、主に検証ルーチンの中の検証部59についての構成を示している。ここでは各構成例の違いを明確にするために、検証部59の中に比較部591や期待値記憶部592があるような構成として示したが、これに限らず期待値記憶部592などは検証部59の外側に構成しても構わない。

【0103】（1）検証部59の構成例の1を図8に示す。この構成例では、検証部59は、期待値記憶部592と、比較部591とを有し、期待値記憶部592には証明データとして期待している期待値 A を記憶している。検証部59への入力には、証明プログラムから受信した証明データ、あるいは認証データ生成時に乱数効果を付与した場合には受信した証明データから乱数効果を除去した証明データが入力される。この入力された証明データ A' と、期待値記憶部592に記憶している期待値 A とを比較部591で比較する。比較の結果、正当と判定された時には、表示部（復号/表示部61）に正当の判定を渡し、表示部はデータを表示する。

【0104】この構成の場合、期待値記憶部592に記憶している期待値 A がプログラム解析などによって窃取されることは、困難ではあっても不可能ではない。期待値 A が窃取されると、乱数効果を付与する際の乱数が予想可能であると、証明プログラムの動作を模倣する装置を構成することが可能となり、なりすましによる不正ア

クセスが可能となる。このようなことを防ぐためには、逆方向への変換が困難な性質を持つ一方向性関数 $h()$ を用いて、期待値記憶部592に記憶する期待値として、 A に一方向性関数 $h()$ を施して得られるデータ $h(A)$ を記憶しておき、検証部591に入力された証明データ A' に対して、一方向性関数 $h()$ を施した結果のデータ $h(A')$ との比較を行うようにすればよい。このように構成することで、万一、期待値記憶部592に記憶している期待値 $h(A)$ が窃取されたとしても、 $h(A)$ から A を計算することは著しく困難であるので、上記のようななりすましを防ぐことができる。

【0105】（2）検証部59の構成例の2を図9に示す。この構成例では、検証部59は、期待値記憶部592と、比較部591と復号鍵記憶部593とを有し、期待値記憶部592には証明データとして期待している期待値 A を記憶している。検証部59への入力には、証明プログラムから受信した証明データ、あるいは認証データ生成時に乱数効果を付与した場合には受信した証明データから乱数効果を除去した証明データが入力される。この入力された証明データ A' と、期待値記憶部592に記憶している期待値 A とを比較部で比較する。比較の結果、正当と判定された時には、復号鍵記憶部593から復号/表示部61に復号鍵 K を渡し、復号/表示部61はこの復号鍵 K を用いて暗号化データを復号し、データを表示する。

【0106】構成例1と同様に、一方向性関数 $h()$ を用いることも可能である。

【0107】（3）検証部59の構成例の3を図10に示す。この構成例では、構成例1と同様に検証部59は、期待値記憶部592と、比較部591とを有するが、期待値記憶部592には期待値として復号鍵 K を記憶している。構成例1と同様に、入力された証明データ K' と、期待値記憶部592に記憶している期待値 K とを比較部591で比較する。比較の結果、正当と判定された時には、復号/表示部61に復号鍵 K' を渡し、復号/表示部61はこの復号鍵 K を用いて暗号化データを復号し、データを表示する。

【0108】（4）検証部59の構成例の4を図11に示す。この構成例では、検証部59は、冗長性検査部594を有している。検証部59への入力には、証明プログラムから受信した証明データ、あるいは認証データ生成時に乱数効果を付与した場合には受信した証明データから乱数効果を除去した証明データが入力される。この入力された証明データ K' を冗長性検査部594で検査する。この方法は、前述したように予め K に冗長性を持たせておき、 K' がその冗長性を持っているかどうかを検査するものである。例えば、国際規格ISO9796などの方法を用いることができる。冗長性検査部594で冗長性の検査に合格すると、冗長性検査部594は復号/表示部61に復号鍵 K' を渡し、復号/表示部61

(13)

特開平11-31130

はこの復号鍵Kを用いて暗号化データを復号し、データを表示する。

【0109】【実施例2】つぎに本発明の実施例2について説明する。本発明の実施例1では、証明データ生成装置11によって生成された証明データが検証用データとアクセス資格認証の特徴情報とに基づいて生成されたデータであることを、証明データ検証装置10の検証ルーチン15が検証し、証明データの正当性が検証されたときに限って、サービスが提供されるサービス提供装置について、インターネットブラウザに、証明データ検証ルーチン15と復号プログラム35とを一体化してプラグイン・モジュールとして組み込んだ例について述べた。実施例1では、検証ルーチン15が受信した証明データから乱数効果を除去した結果が、復号/表示部により復号するための復号鍵になり、その復号鍵が正当なものであるかどうかを判定して、正当なものであるときのみその復号鍵を用いて、暗号化データを復号してサービスを提供するものであった。

【0110】しかし、実施例1のように、証明データから乱数効果を除去した結果を復号鍵として用いる例では、必ずしもその復号鍵の正当性を判定する必要はない。証明データから乱数効果を除去した結果をそのまま復号鍵として用いて、暗号化データを復号することにより、正当な復号鍵である場合には、正しく復号が成功してサービスを提供することが可能になり、正当な復号鍵でない場合には、復号は成功せずに、サービスを提供することができないという結果になるだけである。

【0111】実施例2では、このように検証部のない例について説明する。以下、実施例2では、検証ルーチンという言葉は用いるが、この検証ルーチンには検証部は存在しない。つまり、検証が成功したかどうかを判定する部分は存在しない。暗号化されたコンテンツからアクセスチケット公開鍵(E, n)と認証データKEを取り出し、それらを用いて認証用データを生成して証明プログラムに送信し、証明プログラムから返送された証明データから乱数効果を除去した結果を、復号鍵として復号/表示部に渡す処理を行うものである。

【0112】図12は、実施例2の構成例を示したものである。図12は、図4から検証部59をなくした構成であり、それ以外は図4と同じ構成である。

【0113】動作についても、実施例1で説明したのと同様であり、【ステップ1】～【ステップ7】は同じ処理を行う。以下、【ステップ8】以降について説明する。

【0114】【ステップ8】：ステップ7により検証ルーチンの処理は終了し、検証ルーチンは、前記乱数効果除去部58で計算したK'を復号鍵として復号/表示部61へ渡す。

【0115】【ステップ9】：復号/表示部61は、検証ルーチンの乱数効果除去部58から復号鍵K'を受け

取り、データ分離部56で分離した暗号化されたコンテンツを復号して表示する。証明プログラムにおいて、正当なトークンを持つユーザが正当なアクセスチケットを用いて証明データを生成したときのみ、復号鍵K'は正しい復号鍵になり、暗号化されたコンテンツが正しく復号されて表示される。トークンまたはアクセスチケットが正当でない時には、復号鍵K'は正しい復号鍵とはなり得ず、暗号化されたコンテンツは正しく復号されないため、正しい表示がされないことになる。

【0116】【実施例3】つぎに本発明の実施例3について説明する。図13は本発明の実施例3の構成を示している。この実施例3は証明データ検証側で上記とは異なるプロトコルを用いた例であり、実施例1の図8

(b)で示した検証部の構成要素を、検証部の外に出した構成に近いものである。図4と対応するものは同じ番号で示してある。図13において、81は復号鍵記憶部を表し、コンテンツを復号するための復号鍵Kを検証ルーチンが予め保持している。

【0117】暗号化されたコンテンツの構成は、暗号化されたコンテンツ本体と、アクセスチケット公開鍵とで構成されており、認証データを含む必要はない。

【0118】次に、動作について説明する。以下の説明における変数は、すべて整数である。

【0119】【ステップ1】：ユーザがインターネットブラウザから暗号化されたコンテンツの利用を要求すると、インターネットブラウザは暗号化されたコンテンツのデータタイプを見て、そのデータタイプに関連付けられているプラグインを探してロードし、起動する。対応するプラグインが起動すると、プラグイン中の検証ルーチン15が立ち上がる。この場合のコンテンツとはユーザがインターネットブラウザを通して利用するようものを指し、例えばホームページの表示情報(画像、動画、ハイパードキュメントなど)であったり、Javaアプレットのようなプログラムであったりする。

【0120】【ステップ2】：プラグインの検証ルーチン15は、データ分離部において暗号化されたコンテンツからアクセスチケット公開鍵(E, n)を取り出し、アクセスチケット公開鍵記憶部51に格納する。

【0121】【ステップ3】：次に、検証ルーチン15は、乱数生成部53で乱数rを生成し乱数記憶部54に格納し、乱数rを送信データ(チャレンジ)Cとして、チャレンジCとアクセスチケット公開鍵法数(RSA法数)nとを、証明データ生成側に送信する。この場合、証明用プログラムが返す証明データは、チャレンジCを法数nのもとで、RSA暗号を用いて暗号化したものになるはずである。

【0122】【ステップ4】：証明用プログラムでは、検証ルーチンから送られたチャレンジCとRSA法数nとを認証用データ受信部で受信し、証明データ(レスポンス)Rを以下のようにして生成する。まず、第1演算

(14)

特開平11-31130

部ではアクセスチケット記憶部72から、RSA法数 n をキーにして対応するアクセスチケット t を取得し、RSA法数 n のもとで、式6を実行し中間情報 R' を得る。

【0123】[ステップ5]: 第2演算部75は、ユーザ固有情報記憶部74に記憶されているユーザ固有情報 e を取得し、式7を実行し差分情報 S を得る。

【0124】[ステップ6]: そして、証明データ生成部76は第1および第2演算部75から中間情報 R' および差分情報 S を得て、式8の計算を行い証明データ R を得る。証明データ R は、検証側に送信される。

【0125】[ステップ7]: 検証ルーチン15の検証部59は、受信した証明データ R を取得し、式10の計算を行い乱数記憶部54に記憶されている乱数 r と計算結果 r' とを比較することにより検証を行う。

【0126】

【数10】(10) $r' = RE \bmod n$

乱数 r と計算結果 r' とが等しいとき検証は成功したとみなされ、検証ルーチン15は復号鍵 K を復号/表示部へ渡す。

【0127】[ステップ8]: 復号/表示部61は、検証部59から復号鍵 K を受け取り、データ分離部56で分離した暗号化されたコンテンツを復号して表示する。復号されたコンテンツをインターネットブラウザへ渡して、インターネットブラウザで表示する方法も可能であるが、復号された情報がインターネットブラウザによりコピーされる可能性があるため、安全性の面からは、インターネットブラウザが指定した領域にプラグインが直接表示するほうが望ましい。

【0128】このように、検証ルーチンではユーザが正当な権利を有することのみを検証し、検証が成功した場合に、予め登録されていた復号鍵で暗号化されたコンテンツを復号するようにしてもよい。

【0129】上記第1ないし実施例3で検証ルーチンの部分をソフトウェアプログラムで構成する例を示したが、その場合、コンテンツの復号鍵 K は秘密にしておかなければならない。なぜなら、 K が漏洩してしまうと暗号化されたコンテンツは誰でも復号できることになってしまい、コンテンツの不正利用を許してしまうこととなる。従って、検証ルーチンは何らかの方法で内部データを保護する必要がある。そのような方法として、プログ

(12)

$$F(x, y, z) = h(x | y | z)$$

上式中の記号はすべて整数であり、実施例1と同様に、 n はRSA法数、 D はアクセスチケット秘密鍵、 e はユーザ固有情報を表す。 L は利用制御情報であり、関数 $F()$ は一方方向性関数である。

【0135】図14を参照してさらに本実施例について詳細に説明する。図14は、本発明の実施例4の構成例を具体的に示すものである。図14の左半分、つまりプラグインおよび検証ルーチン側は、実施例1の図4と同

ラムをマシン語にコード化する際に内部データやプログラム手順が解析し難くなるように難読化する方法がある。これらの技術は、村上隆徳ら「プログラムコードの難読化について」、電子情報通信学会技術研究報告(I E I C E Technical Report)情報セキュリティ、I SEC95-25(1995)等で紹介されている。また、ソフトウェア的手法以外に、検証ルーチンと復号プログラムとを1つのハードウェアで構成する方法を用いてもよい。その場合は、専用のハードウェアやPCカードおよびICカード等で構成することができる。また、検証ルーチン、証明データ生成部および復号/表示部すべてを1つのハードウェアで構成することも可能である。

【0130】[実施例4] つぎに本発明の実施例4について説明する。本実施例では、利用制御情報を用いた構成例について説明する。利用制御情報は、証明データの生成を制御するための制御情報であり、またサービスを提供する条件を記述する制御情報であり、アクセスチケットとともに配布される。制御情報は、例えば、サービスを提供する期限、料金額、回数、時間などを記述することができ、証明データを生成するときに、これらの条件をチェックして、条件に合致しないときには証明データの生成を行わないようにして、サービスの提供をストップすることができる。これ以外にも制御情報には、役職、性別、年齢などのようなユーザの属性を記述しておいて、トークン中に保持されているユーザの属性と比較して、証明データの生成を制御することも可能である。

【0131】以下では、制御情報として利用期限を用いたときの説明と、料金額を用いたときの説明を簡単に述べる。

【0132】本実施例では、アクセスチケット t は次の式11に基づいて生成されるデータである。

【0133】

【数11】

$$(11) \quad t = D - F(n, e, L)$$

三変数関数 $F(x, y, z)$ は関数値が衝突しにくい三変数関数であり、例えば前述の一方方向性ハッシュ関数 h を利用して式13のように定めることができる。

【0134】

【数12】

$$F(x, y, z) = h(x | y | z)$$

である。

【0136】証明用プログラム32は、証明用データ受信部71、アクセスチケット記憶部72、第1演算部73および証明データ生成部76とで構成され、トークン33はユーザ固有情報記憶部74、第2演算部75および利用制御情報判定部77とで構成される。

【0137】アクセスチケット記憶部72は、RSA法数 n と、アクセスチケット t に加えて、利用制御情報 L

7
745

(15)

特開平11-31130

とを組にして記憶している。利用制御情報判定部77は、アクセスチケット記憶部72から渡された利用制御情報Lの条件を判定し、判定の結果正しいと判定したときのみ、利用制御情報Lを第2演算部75に渡す。第2演算部75では、利用制御情報判定部77から利用制御情報Lを渡されたときのみ、式13に基づいて差分情報Sを計算し、証明データ生成部76に送る。

【0138】

【数13】

$$(13) \quad S = CF(n, e, L) \bmod n$$

以下では、利用制御情報として利用期限を用いたときについて説明する。利用制御情報として利用期限を持つときには、利用制御情報Lの値は、例えば199712312400のような値である。この場合、この値は利用期限が1997年12月31日24:00までということを表している。このような数字ではなく、ある日時からの相対的な秒数で表すなどにしてもかまわない。

【0139】トークン中の利用制御情報判定部77は、時計を持ち、アクセスチケット記憶部72から渡された利用制御情報Lと現在の時刻とを比較する。そして比較の結果、利用制御情報Lの値が現在の時刻より後である場合には、正しいと判定し、利用制御情報Lを第2演算部75に渡す。第2演算部75では、利用制御情報判定部77から利用制御情報Lを渡されたときのみ、式13に基づいて差分情報Sを計算し、証明データ生成部76に送る。

【0140】以降、実施例1と同様に、証明データ生成部76で式8を用いて証明データRを計算し、検証ルーチン15の乱数効果除去部58では、証明データ受信部57で受信した証明データRを取得し、乱数記憶部54に記憶されている乱数rとにより、式9の計算を行いK'を得る。

【0141】正しいアクセスチケットtと、正しいユーザ固有情報eと、正しい利用制御情報Lとを用いて計算がなされたときに限って、K' = Kが成り立ち、検証ルーチン15の検証部により正しいとの判定が下されて、サービスが提供される。利用制御情報Lの利用期限がきれているアクセスチケットを使おうとして、何者かが、アクセスチケット記憶部72に記憶されている利用制御情報Lを改竄したとしても、アクセスチケットtを改竄することはできないため、証明データ生成部76で式8を用いて生成された証明データRは正しい値にはなり得ず、不当にサービスの提供を受けることはできない。

【0142】利用制御情報Lがサービスの利用額であるときには、例えば利用制御情報Lの値として、1回100円の意味で、100という数字が与えられている。

【0143】トークンは、例えばプリペイドの残高情報を記憶するプリペイド残高記憶部を有し、トークン中の利用制御情報判定部77は、利用制御情報Lとプリペイド残高とを比較して、プリペイド残高の方が大きいとき

に、正しいと判定し、プリペイド残高から利用制御情報L分に相当する値を減額して、利用制御情報Lを第2演算部75に渡す。以下の処理は同様である。

【0144】また、プリペイド残高記憶部のかわりに、利用履歴記憶部を有し、トークン中の利用制御情報判定部77は、利用制御情報Lの値を時刻などの情報とともに利用履歴記憶部に記録して、利用制御情報Lを第2演算部75に渡すようにしてもよい。この場合には、時々利用履歴記憶部に記憶されている利用履歴を回収して、相当する金額を支払うなどの処理を行う。

【0145】このように、ここで示した例以外にも、利用制御情報判定部77により利用制御情報Lをチェックした後で利用制御情報Lを第2演算部75に渡すように構成することで、さまざまな利用制御を行うことが可能になる。

【0146】【実施例5】つぎに本発明の実施例5について説明する。実施例5は、衛星放送を利用してカプセル化されたコンテンツを配信して、サービスを提供する例である。ここで、カプセル化とは暗号化等を施すことによりコンテンツをそのままでは利用できないようにすることを指す。図15に衛星放送を利用したサービス提供システムの概略図を示す。カプセル化されたコンテンツは衛星放送を利用して、各ユーザに配信される。ユーザは衛星電波を衛星アンテナで受信し受信機100に入力する。受信機では本発明のサービス提供装置が実装しており、検証が成功した場合にコンテンツを利用できるようになっている。

【0147】ここで提供されるコンテンツは、映画、音楽、テレビ番組、ソフトウェア、写真、文献、ニュース等さまざまなものが考えられる。それぞれのコンテンツは受信機100に接続されたテレビ・ビデオ200、オーディオ機器300、コンピュータ(PC)400等で利用される。ここでは、受信機100とサービス利用機器が分割されている例について説明するが、受信機100が内蔵されたサービス利用機器でも同様に説明できる。

【0148】カプセル化されたコンテンツの構造を図16に示す。カプセル化されたコンテンツは、コンテンツヘッダと暗号化されたデータとに分類される。コンテンツヘッダはコンテンツの識別をするためのラベルと公開鍵(E, n)および暗号化された復号鍵を有している。暗号化されたデータは前記の実施例で暗号化されたコンテンツ本体に相当する。

【0149】図17は図15における受信機100の構成を具体的に示した例である。受信機100の各回路はマイクロコンピュータによってコントロールされている。衛星アンテナからの衛星信号は、まず受信機100のチューナ101に入力される。チューナ101は受信機100のパネルもしくはリモコンによりユーザが選択したチャンネルのデータを抽出する。誤り訂正回路/デス

(16)

特開平11-31130

クランブル回路102は、抽出されたデータをコンテンツとして復元し、データ・コントロール回路103に入力する。データ・コントロール回路103では、コンテンツがカプセル化されているかどうかをコンテンツラベルで識別し、コンテンツがカプセル化されていない場合は、そのまま出力側へ渡す。コンテンツがカプセル化されている場合には、コンテンツを検証/復号回路104に入力する。検証/復号回路104では、これまでの実施例で示した検証ルーチンにより正当性を検証することが可能であるが、実施例5では、別の方法を示して説明する。この方法の詳細については図18を参照して説明する。なお、復号されたデータはデマルチプレクス回路105を介してビデオデコーダ106またはオーディオデコーダ107の送られて対応する信号として利用機器に供給される。

【0150】図18に、実施例5の検証手順（プロトコル）を示す。実施例1と同様の機能を有する部分は同じ番号で示してある。

【0151】実施例5におけるアクセスチケットtは式14に基づいて生成されるデータである。

【0152】

$$[数14] \quad (14) \quad t = D - F(n, e)$$

上式中の記号はすべて整数であり、以下を表す。（実施例1の式参照）

nはRSA法数、即ち十分大きな二つの素数p、qの積である（ $n = pq$ ）。 $\phi(n)$ はnのオイラー数、即ち、 $p-1$ と $q-1$ の積である（ $\phi(n) = (p-1)(q-1)$ ）。eはユーザ固有情報を表し、ユーザ毎に異なる数で、ユーザを識別するために用いる。Dはアクセスチケット秘密鍵を表し、法数nのもとでのRSA秘密鍵であり、式2を満たす。ここで、 $gcd(x, y)$ は二数x、yの最大公約数を表す。

【0153】式(2)によって表現される性質は、式3を満たす数Eが存在することを保証する。Eはアクセスチケット公開鍵と呼ぶ。

【0154】二変数関数 $F(x, y)$ は関数値が衝突しにくい二変数関数であり、例えば前述の一方方向性ハッシュ関数hを利用して式15のように定めることができる。

【0155】

【数15】

$$(15) \quad F(x, y) = h(x | y)$$

以下図を用いて、実施例5を詳細に説明する。図17における検証/復号回路104は図18では38で示される。検証/復号回路38は検証ルーチン15と復号部61とからなり、ASIC(application specific integrated circuit)等で実現されることで、復号の高速処理や検証ルーチンの安全性が保証される。もちろん検証/復号回路38をソフトウェアプログラムで実現することも可能であ

る。また、より安全性を高めるために、前述した耐タンパ特性を有するハードウェアで構成してもよい。検証/復号回路では、データ・コントロール回路より受け取ったカプセル化されたコンテンツをデータ分離部56でコンテンツヘッダと暗号化されたデータとに分離し、公開鍵(E, n)をアクセスチケット公開鍵記憶部51に、暗号化された復号鍵KEを認証データ記憶部52に、暗号化されたデータを復号部61にそれぞれ格納する。そして検証/復号回路は内部の乱数生成部で乱数を生成し乱数記憶部54に記憶する一方で、送信データ計算部において送信データCを実施例1と同様に式5に基づいて計算する。

【0156】このようにして計算した送信データCは、法数nと一緒に証明プログラムに送信される。

【0157】証明プログラムの第1演算部73および証明データ生成部76の演算はマイクロコンピュータで実行され、アクセスチケットはEPROM(erasable programmable read only memory)等に記憶されている。認証データは受信したnを基にアクセスチケット記憶部72から、対応するアクセスチケットtを選択し、認証データ受信部71から受け取ったRSA法数nのもとで、式16を実行し中間情報R'を得る。

【0158】

【数16】

$$(16) \quad R' = Ct \bmod n$$

トークンはICカードにより実現され、ユーザ固有情報記憶部74および第2演算部75を有し、マイクロコンピュータから認証用データを受け取って式17を実行し差分情報Sを得る。

【0159】

【数17】

$$(17) \quad S = CF(n, e) \bmod n$$

そして、証明プログラムの証明データ生成部75は第1および第2演算部73、75から中間情報R'および差分情報Sを得て、式18の計算を行い証明データRを得る。

【0160】

$$[数18] \quad (18) \quad R = R' S \bmod n$$

このようにして得られた証明データRは、検証/復号回路の証明データ受信部57に送信される。

【0161】検証ルーチン15の乱数効果除去部58は、データ受信部57で受信した証明データRを取得し、乱数記憶部54に記憶されている乱数rとにより、式19の計算を行い復号鍵Kを得る。

【0162】

$$[数19] \quad (19) \quad K = Rr^{-1} \bmod n$$

このときKに冗長性をもたせ、その部分に特定の値を持たせておくことで、復号鍵Kが正しく復号されたかどうかを検証部59で検証するようにしてもよい。得られた

(17)

特開平11-31130

復号鍵Kは復号部61に入力され、復号部61では暗号化されたデータを復号鍵Kを用いて復号しコンテンツとして出力する。

【0163】出力されたコンテンツは、デジタルデータとしてPCで利用されたり、映像情報やオーディオ情報として利用されたりする。

【0164】図19に、本実施例のサービス提供装置の概観図を示す。図に示すようにサービス提供装置はテレビに接続されている。図には示していないがサービス提供装置は衛星アンテナに接続されており、衛星放送を受信する一方、モデムを通してネットワークに接続されており、衛星放送で受信したカプセル化されたコンテンツを利用するためのアクセスチケットを取得できるようになっている。図19(a)に示すように、コンテンツが暗号化されている場合はトークンをサービス提供装置に挿入していない場合は、ユーザは映像を観ることができない。そこで、ユーザは正当なアクセスチケットを取得してサービス提供装置にトークンを挿入すると、図19(b)に示すように映像を見ることができるようになる。

【0165】このように、本発明では、コンテンツを1つの暗号鍵で暗号化して提供しているにもかかわらず、各ユーザ毎にカスタマイズされたアクセスチケットとユーザ固有情報を格納したトークンを両方有しないとサービスを利用することができないようになっている。従ってコンテンツのプロバイダ(提供者)は、コンテンツを暗号化して衛星放送のようなマスメディアを利用して提供することが可能であり、また、アクセスチケットとトークンとによりユーザごとの確実な利用管理を行うことが可能である。

【0166】【実施例6】つぎに本発明の実施例6について説明する。上記はコンテンツごとにカプセル化した場合について記述したが、これ以外の応用例として、衛星放送の放送チャネルについては同じ暗号化を施し、視聴時間を管理することでコンテンツの利用を制限したい場合などがある。このようなサービスはアクセスチケットを式20で表現することで実現される。

【0167】

【数20】(20) $t = D - F(n, e, L)$
ここで、Lは利用制御情報であり、利用期限を表す。三変数関数 $F(x, y, z)$ は関数値が衝突しにくい三変数関数であり、例えば前述の一方方向ハッシュ関数hを利用して式21のように定めることができる。

【0168】

【数21】

(21) $F(x, y, z) = h(x | y | z)$

図20に利用制御情報の構成例を示す。図に示すとおり利用制御情報Lは利用開始時刻、利用終了時刻および利用料金とで構成される。利用料金はトークンがプリペイド機能を有する場合にのみ必要で、プリペイド機能を使

わない場合は省略することができる。図21に利用制御情報Lを用いた場合の検証プロトコルを示す。ここで図18と同様の機能のものは同じ番号で示してある。

【0169】以下、図を用いて実施例6を詳細に説明する。検証/復号回路では、データ・コントロール回路より受け取ったカプセル化されたコンテンツをデータ分離部56でコンテンツヘッダと暗号化されたデータとに分離し、公開鍵(E, n)をアクセスチケット公開鍵記憶部51に、暗号化された復号鍵KEを認証データ記憶部52に、暗号化されたデータを復号部61にそれぞれ格納する。そして検証/復号回路は内部の乱数生成部で乱数を生成し乱数記憶部54に記憶する一方で、送信データ計算部において送信データCを式15に基づいて計算する。

【0170】このようにして計算した送信データCは、法数nと一緒に証明プログラムに送信される。

【0171】証明プログラムの第1演算部73および証明データ生成部76の演算はマイクロコンピュータで実行され、アクセスチケットはEPROM(erasable programmable read only memory)等に記憶されている。認証データは受信したnを基にアクセスチケット記憶部72から、対応するアクセスチケットtと利用制御情報Lを選択し、認証データ受信部71から受け取ったRSA法数nのもとで、式16を実行し中間情報R'を得る。

【0172】トークンは、ユーザ固有情報記憶部74、第2演算部75を有し、さらに、プリペイド度数とトークン時刻データを有している。トークンは、マイクロコンピュータから認証用データと利用制御情報Lを受け取り、利用制御情報中の有効期限がトークン時刻と矛盾しないかどうかを検証する。すなわち、利用開始時刻 \leq トークン時刻 \leq 利用終了時刻となっている場合に検証が成功したとみなされる。有効期限の検証に成功したら、トークンの度数が利用制御情報L内の利用度数以上残っていることを確認し、残っていればトークンの度数から利用制御情報L内の利用度数分を減算する。有効期限の検証に失敗した場合と、度数が足りない場合は処理を行わずエラーを返す。上記の検証が成功した場合は、式22を実行し差分情報Sを得る。

【0173】

【数22】

(22) $S = CF(n, e, L) \bmod n$

そして、証明プログラムの証明データ生成部75は第1および第2演算部73、75から中間情報R'および差分情報Sを得て、式18の計算を行い証明データRを得る。このようにして得られた証明データRは、検証/復号回路の証明データ受信部57に送信される。

【0174】検証ルーチン15の乱数効果除去部58は、データ受信部57で受信した証明データRを取得し、乱数記憶部54に記憶されている乱数rとにより、

7
26

(18)

特開平11-31130

式19の計算を行い復号鍵Kを得る。ここで、もしトークンで用いた利用制御情報が改ざんされていた場合は、正確な復号鍵を取り出すことができない。このときKに冗長性をもたせ、その部分に特定の値を持たせておくことで、復号鍵Kが正しく復号されたかどうかを検証部59で検証するようにしてもよい。得られた復号鍵Kは復号部61に入力され、復号部61では暗号化されたデータを復号鍵Kを用いて復号しコンテンツとして出力する。

【0175】出力されたコンテンツは、デジタルデータとしてPCで利用されたり、映像情報やオーディオ情報として利用されたりする。

【0176】この実施例では、トークンに時刻を持たせているが、ICカードを用いる場合は内部に時計が無いので、トークン時刻の正当性を保証することが必要となる。

【0177】このようにすることで、ユーザはアクセスチケットを利用制御情報中の有効期限内でないと利用できず、1つのチャンネルのコンテンツが同じ暗号鍵で暗号化してあったとしても、時間毎に利用権を設定することができ、ペイパービュー等の機能を実現することも可能である。

【0178】なお、本発明は上述の実施例に限定されるものではなく、例えば、コンテンツの利用は、種々の記録媒体、通信媒体、放送媒体を介して行える。インターネット、衛星放送の他に、種々の通信媒体、放送媒体を利用する場合に適用できる。例えば、通常の電話網、データ通信網、TCP/IP接続による通信カラオケのサービスの提供にも適用できる。

【0179】

【発明の効果】以上説明したように、本発明によれば、証明用補助データ（アクセスチケット）を導入することにより、アクセス資格認証の特徴情報とユーザ固有情報とを独立させることができ、従って、プロテクト側も、ユーザ側も1つの固有情報を準備しておけば済む。アクセスチケットは、特定のユーザ固有情報とアクセス資格認証の特徴情報とに基づいて計算されるデータであり、またユーザ固有情報を知らずにアクセスチケットからアクセス資格認証の特徴情報を計算することは少なくとも計算量適に不可能である。そして、ユーザ固有情報とアクセスチケットの正しく組み合わせられた場合にのみ、サービスを提供（コンテンツを復号）するので、ユーザは予めユーザ固有情報を所持し、サービス提供者はユーザが所持するユーザ固有情報とは独立にアクセス資格認証の特徴情報を用意することができる。従って、例えばコンテンツを1つの暗号鍵で暗号化した場合でも、所望のユーザだけにアクセス権を設定することが可能となり、暗号化したコンテンツをユーザ毎に用意する必要がなくなる。

【図面の簡単な説明】

【図1】 本発明の原理的な構成例を示すブロック図である。

【図2】 実施例1の構成例の概要を示すブロック図である。

【図3】 実施例1のユーザが用いる計算機の概略図である。

【図4】 実施例1の構成例の詳細なブロック図である。

【図5】 実施例1の暗号化されたコンテンツの構成例1である。

【図6】 実施例1の暗号化されたコンテンツの構成例2である。

【図7】 実施例1の暗号化されたコンテンツの構成例3である。

【図8】 実施例1の検証部における処理の構成例である。

【図9】 実施例1の検証部における処理の構成例である。

【図10】 実施例1の検証部における処理の構成例である。

【図11】 実施例1の検証部における処理の構成例である。

【図12】 実施例2の構成例の詳細なブロック図である。

【図13】 実施例3の構成例の詳細なブロック図である。

【図14】 実施例4の構成例の詳細なブロック図である。

【図15】 実施例5の概略図である。

【図16】 実施例5のカプセル化されたコンテンツの構成図である。

【図17】 実施例5の構成例の詳細なブロック図である。

【図18】 実施例5の構成例の詳細なブロック図である。

【図19】 実施例5の構成例の図である。

【図20】 実施例6の利用制御情報の構成図である。

【図21】 実施例6の構成例の詳細なブロック図である。

【符号の説明】

- 10 証明データ検証装置
- 11 証明データ生成装置
- 12 アクセスチケット生成装置
- 13 アクセスチケット（証明用補助データ）
- 14 アクセス資格認証の特徴情報
- 15 検証ルーチン
- 16 ユーザ固有情報
- 17 証明データ生成プログラム
- 18 認証用データ
- 19 証明データ

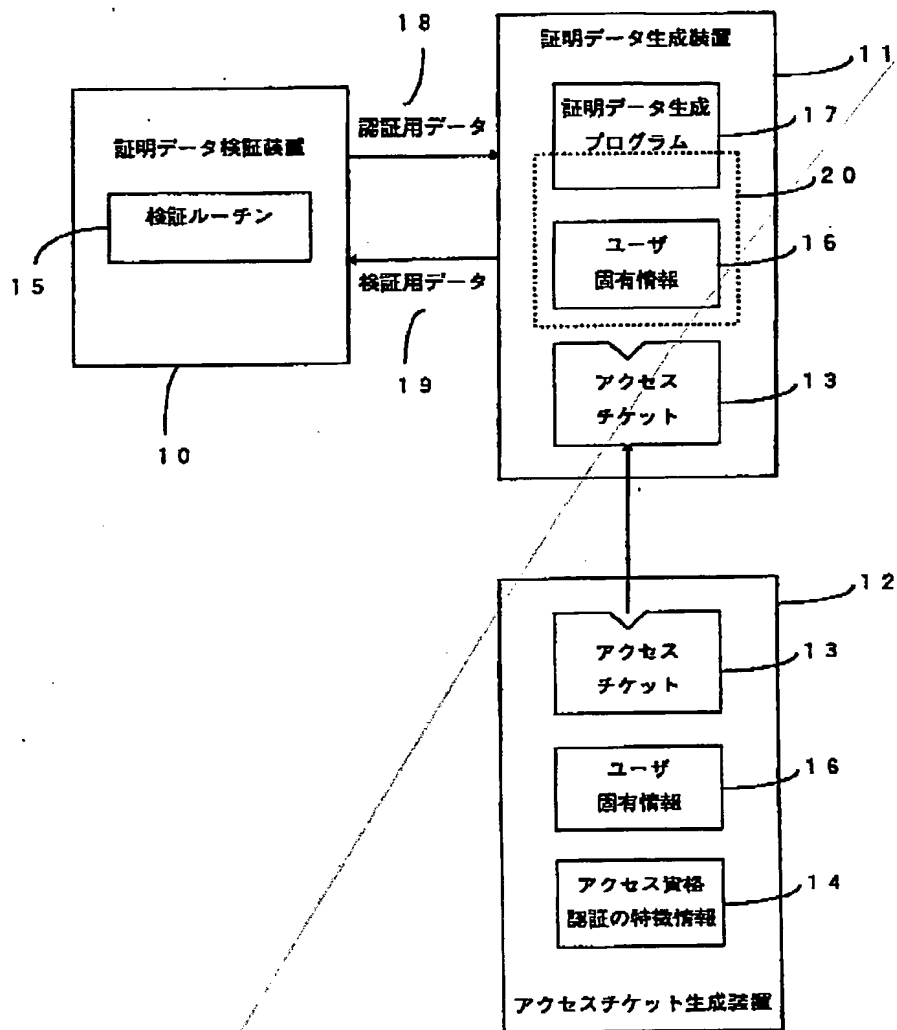
(19)

特開平11-31130

20 耐タンパー装置
30 計算機
31 インターネットブラウザ
32 証明用プログラム

33 トークン
34 コンテンツ
35 複号プログラム
38 プラグイン (プラグイン・モジュール)

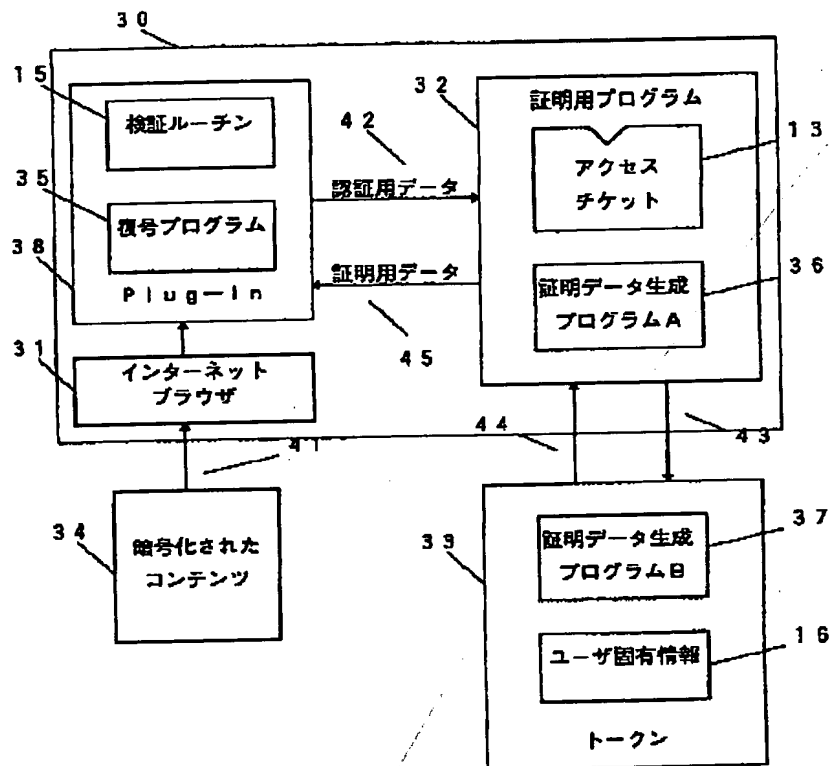
【図1】



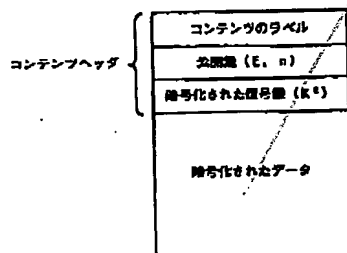
(20)

特開平11-31130

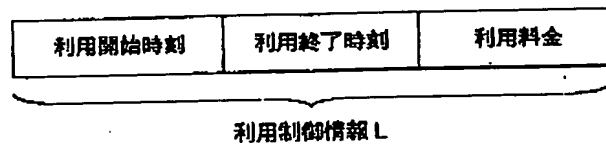
【図2】



【図14】



【図18】

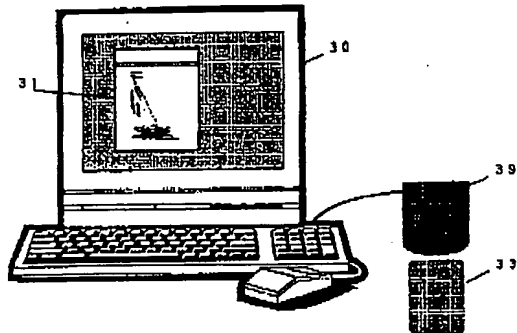


利用制御情報の構成図

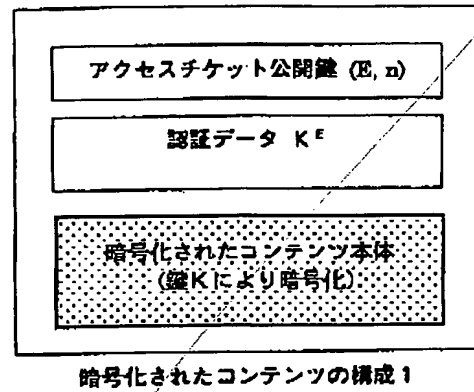
(21)

特開平 11-31130

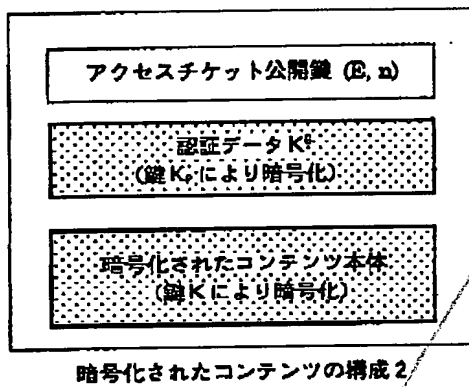
【図 3】



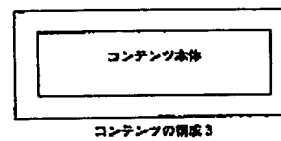
【図 5】



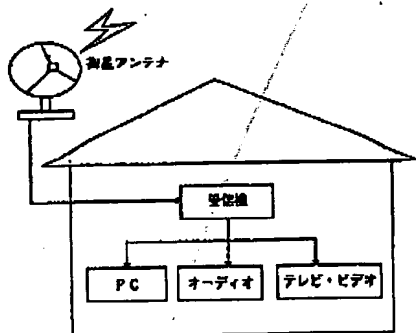
【図 6】



【図 7】



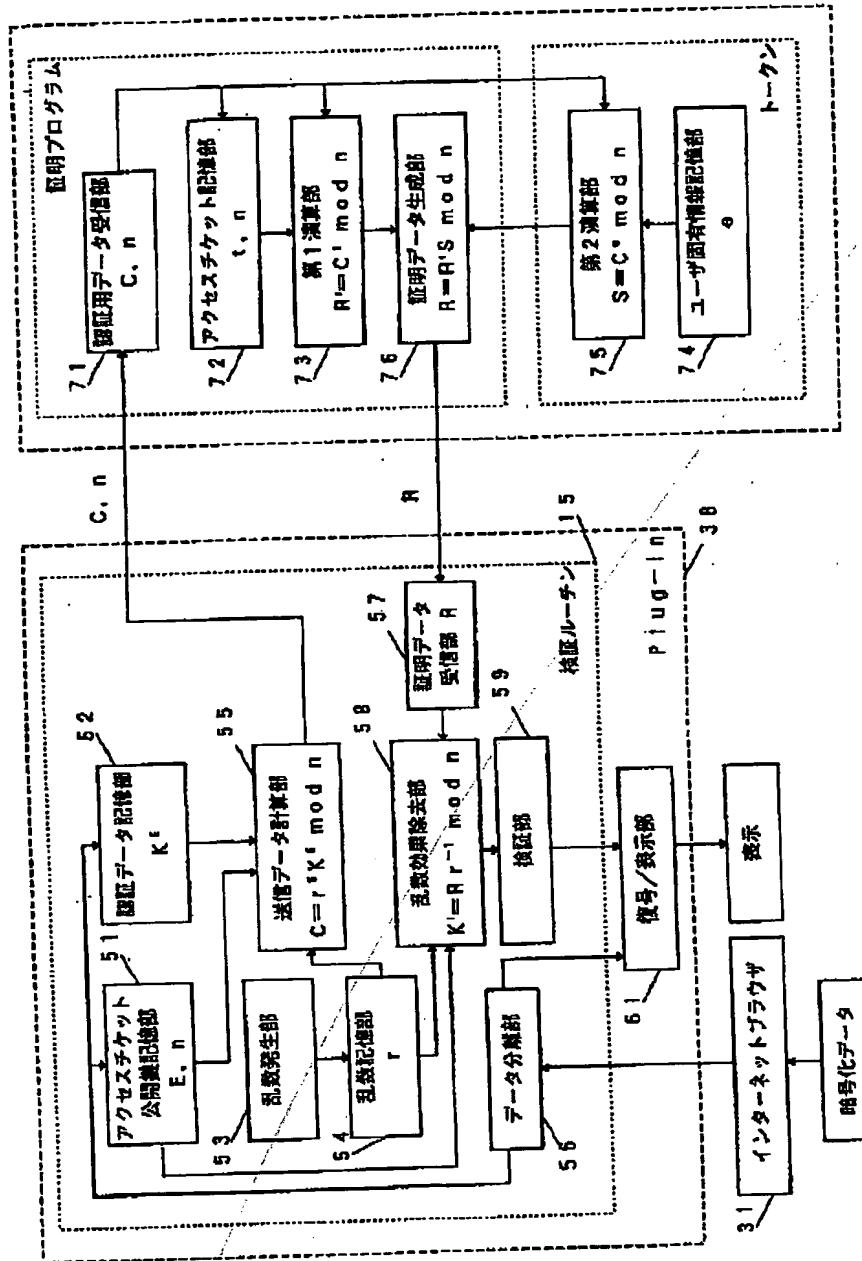
【図 13】



(22)

特開平11-31130

【図4】

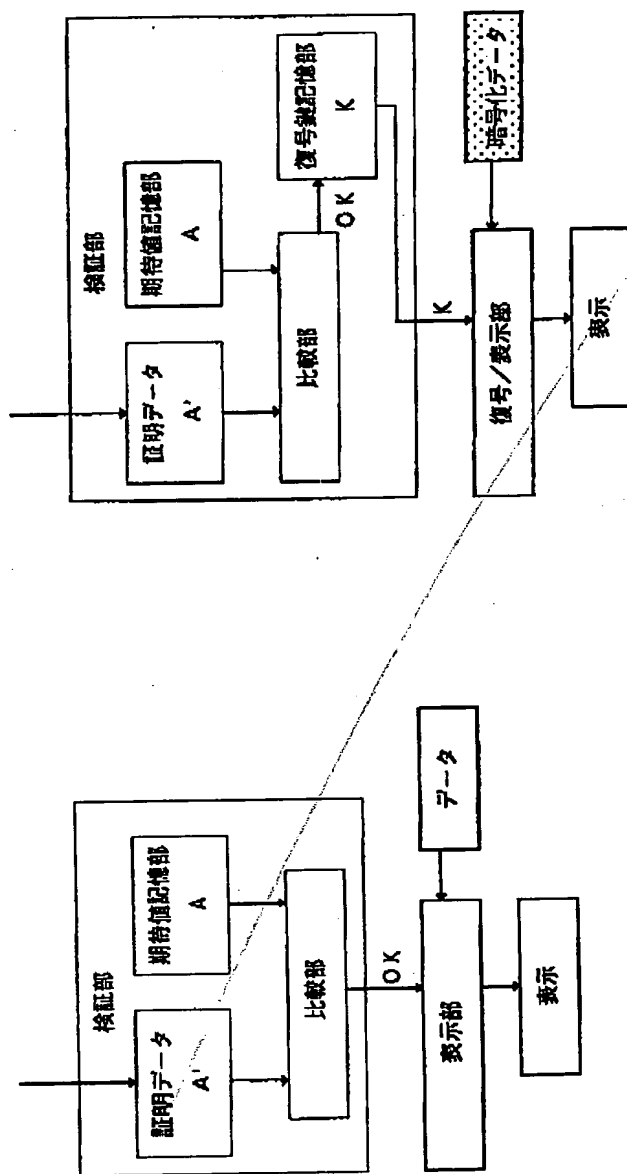


第1の実施例の詳細な構成例

(23)

特開平11-31130

【図8】



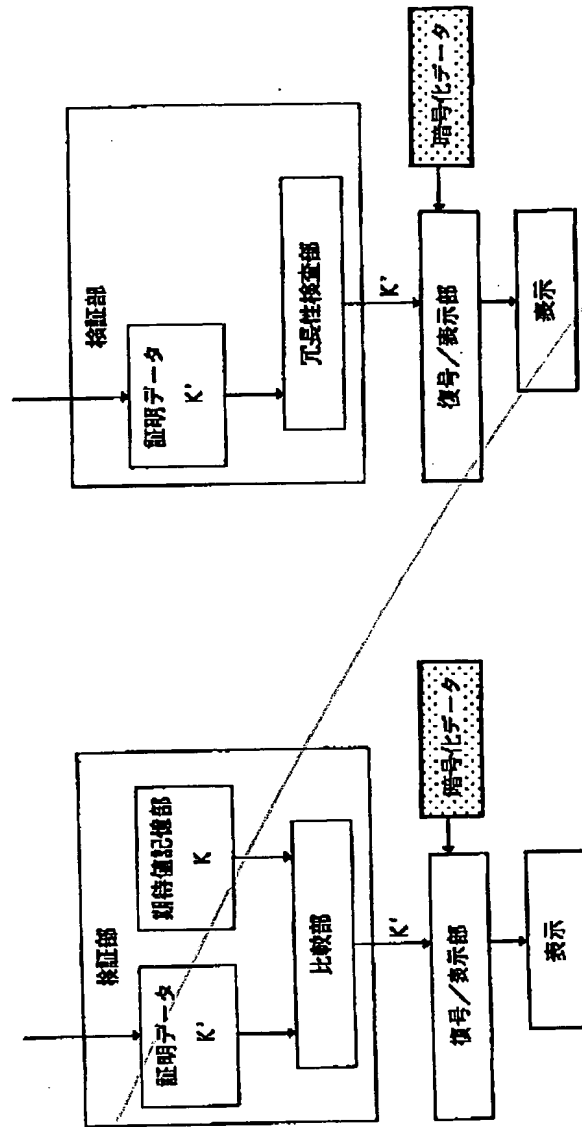
(b) 検証部の構成 2

(a) 検証部の構成 1

(24)

特開平 11-31130

【図9】



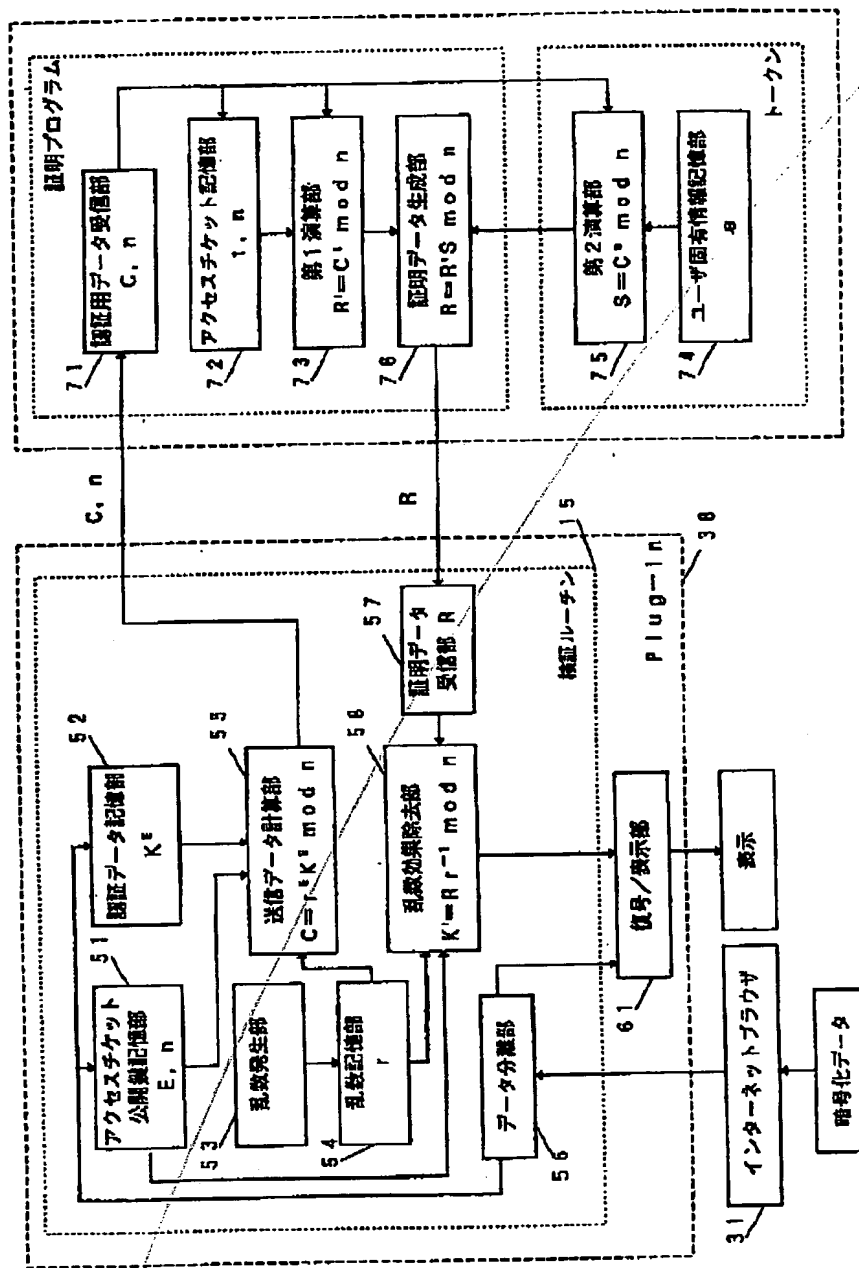
(d) 検証部の構成 4

(c) 検証部の構成 3

(25)

特開平11-31130

【図10】

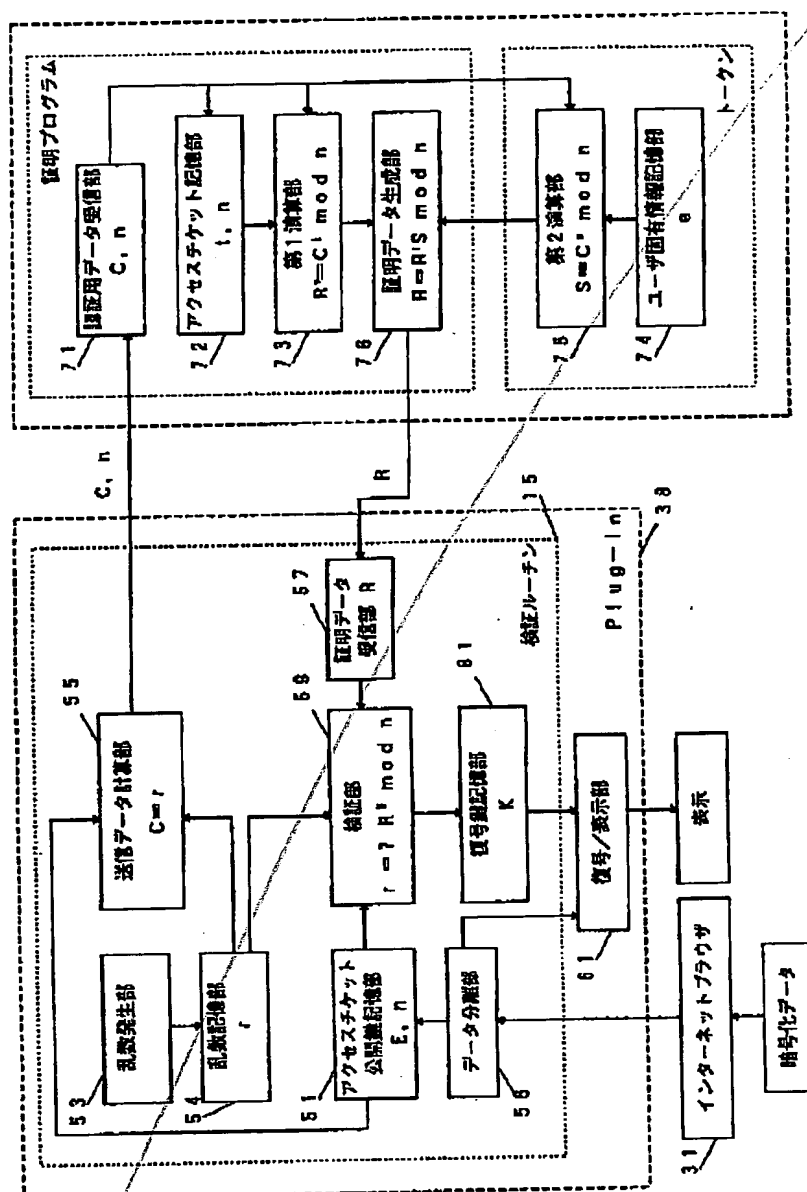


第2の実施例の構成例

(26)

特開平 1 1 - 3 1 / 1 3 0

【图 1-1】

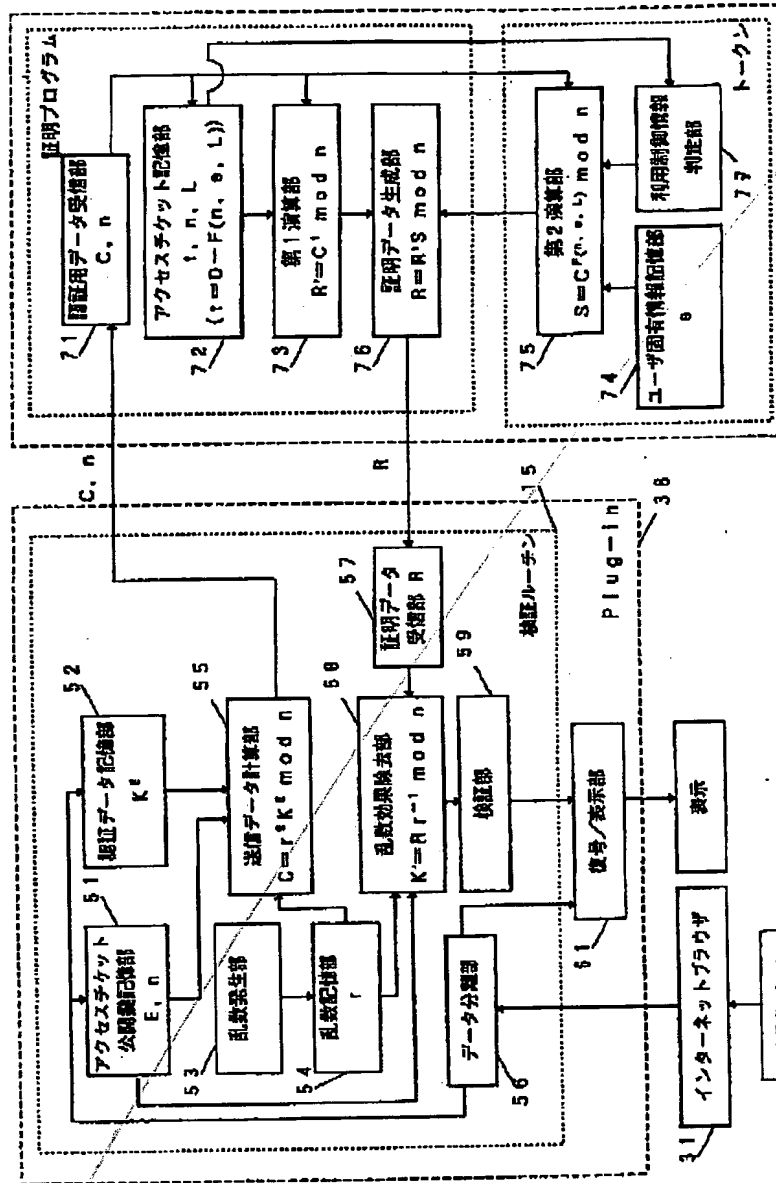


所定数の算出の算式を算式

(27)

特開平11-31130

【図12】



第4の実施例の構成図

(28)

特開平11-31130

【図15】

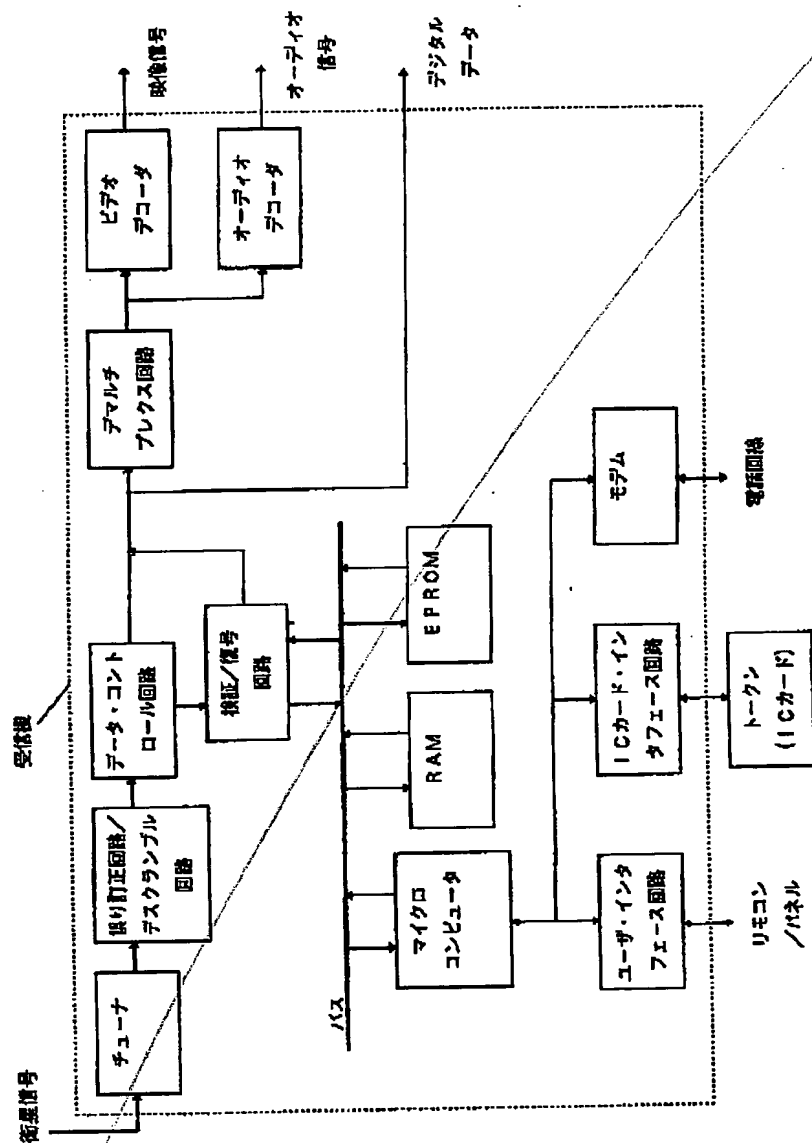
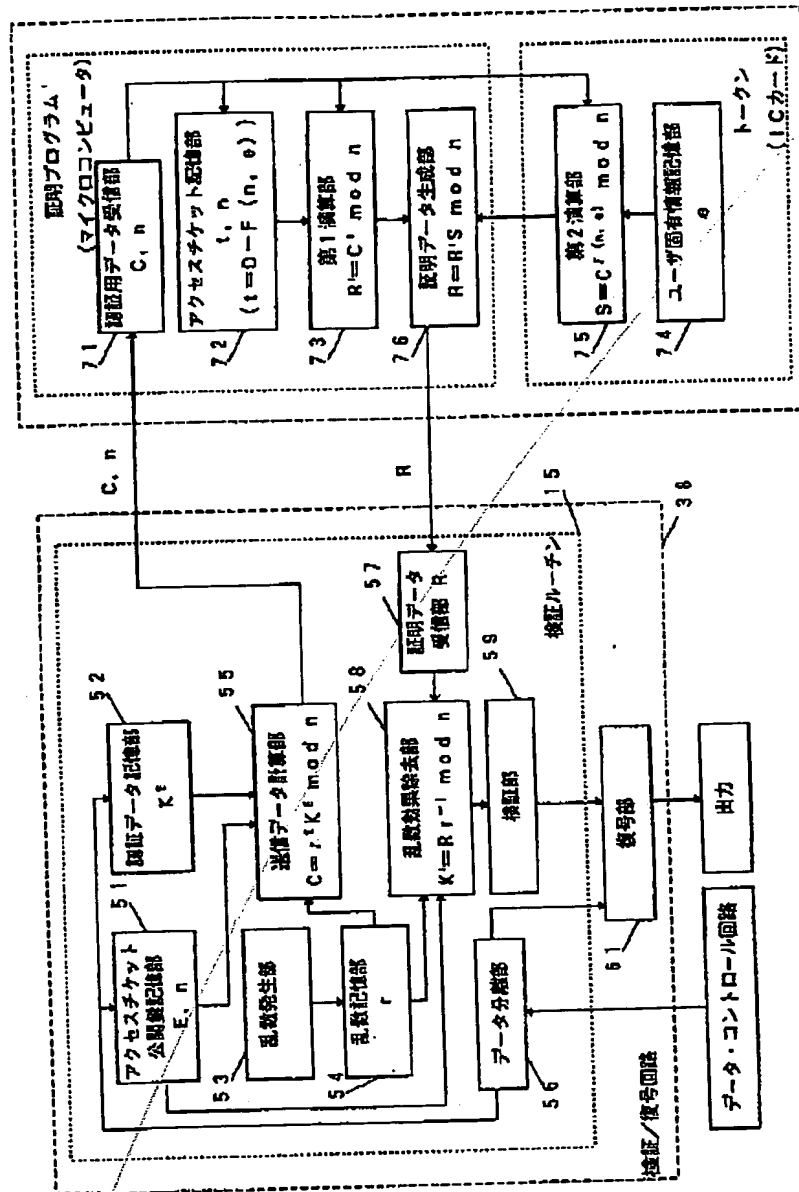


図15の実施例の構成図

(29)

特開平11-31130

【図16】

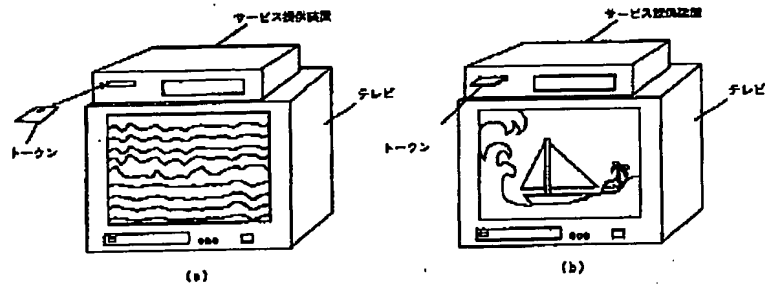


第6の実施例の構成図

(30)

特開平11-31130

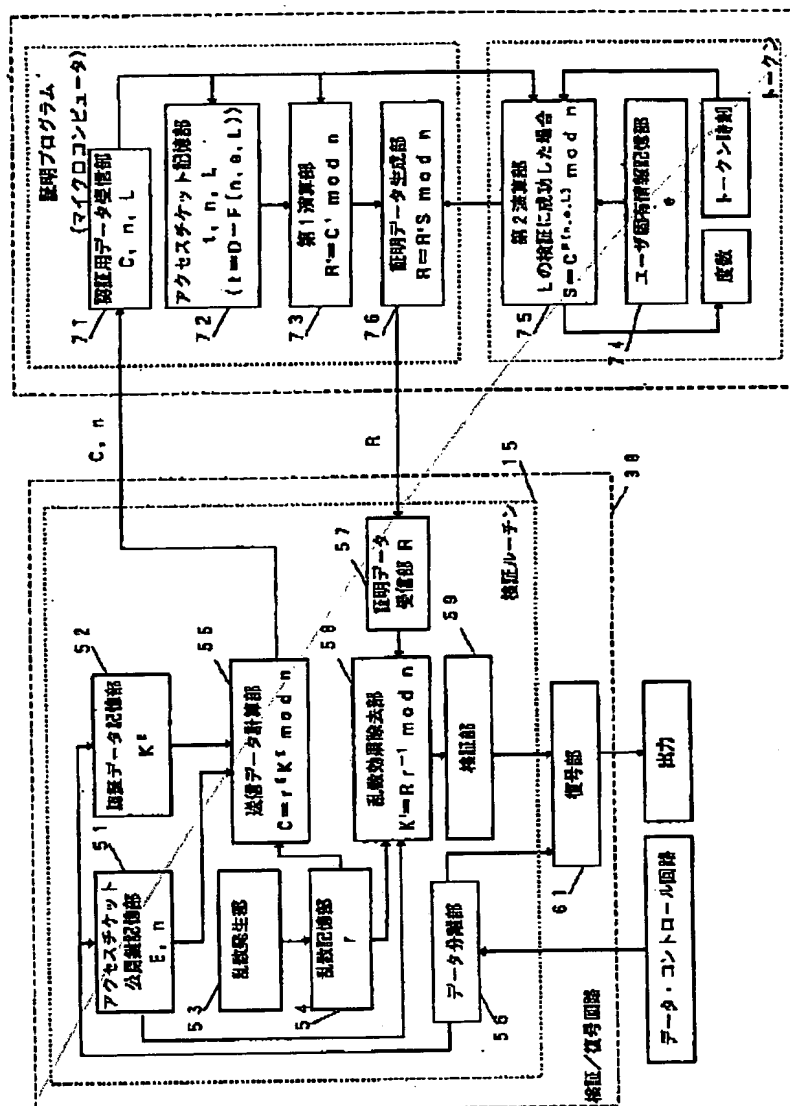
【図17】



(31)

特開平11-31130

【図19】



第6の実施例の構成図

【手続補正書】

【提出日】平成9年10月29日

【手続補正1】

【補正対象書類名】図面

【補正対象項目名】全図

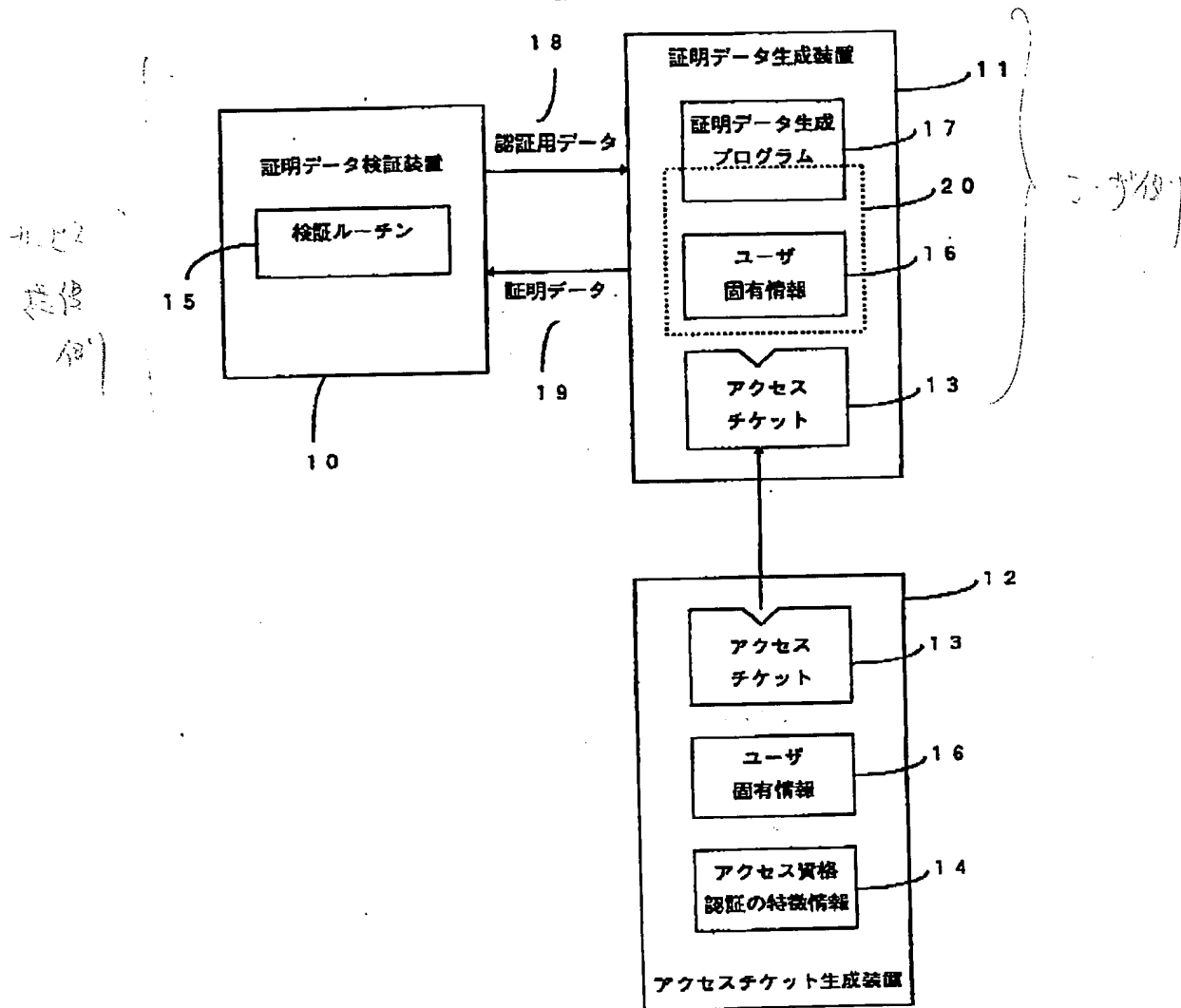
【補正方法】変更

【補正内容】

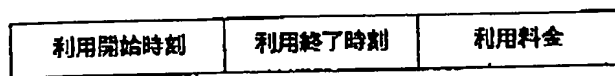
(32)

特開平11-31130

【図1】



【図20】



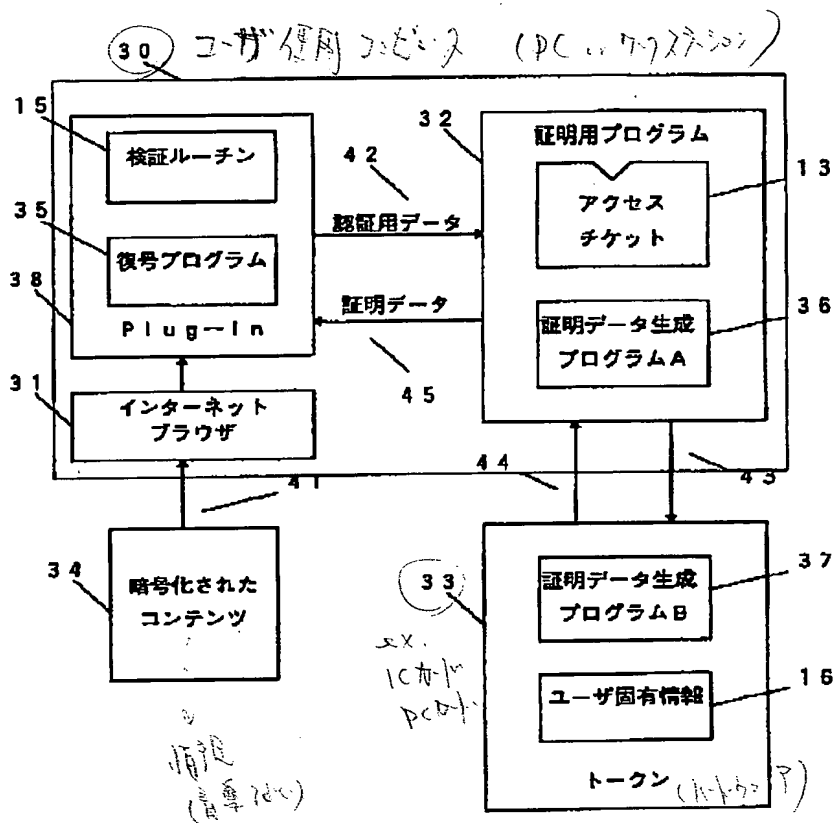
利用制御情報L

利用制御情報の構成図

(33)

特開平11-31130

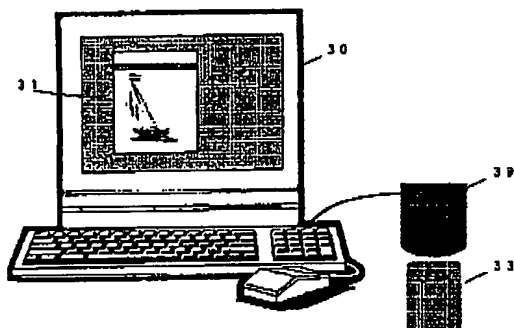
【図2】



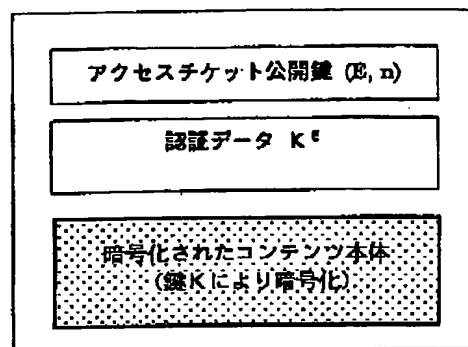
(34)

特開平11-31130

【図3】

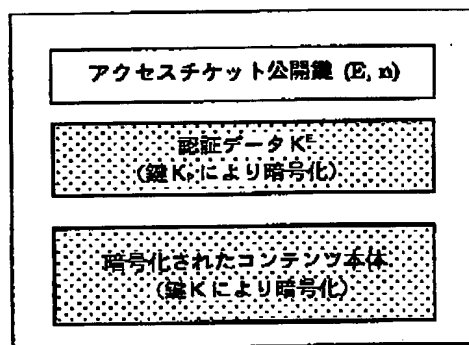


【図5】



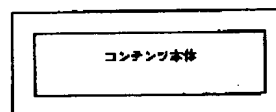
暗号化されたコンテンツの構成1

【図6】



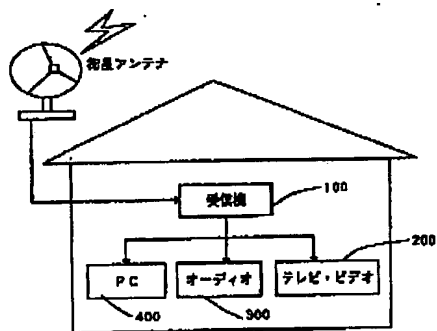
暗号化されたコンテンツの構成2

【図7】



コンテンツの構成3

【図15】

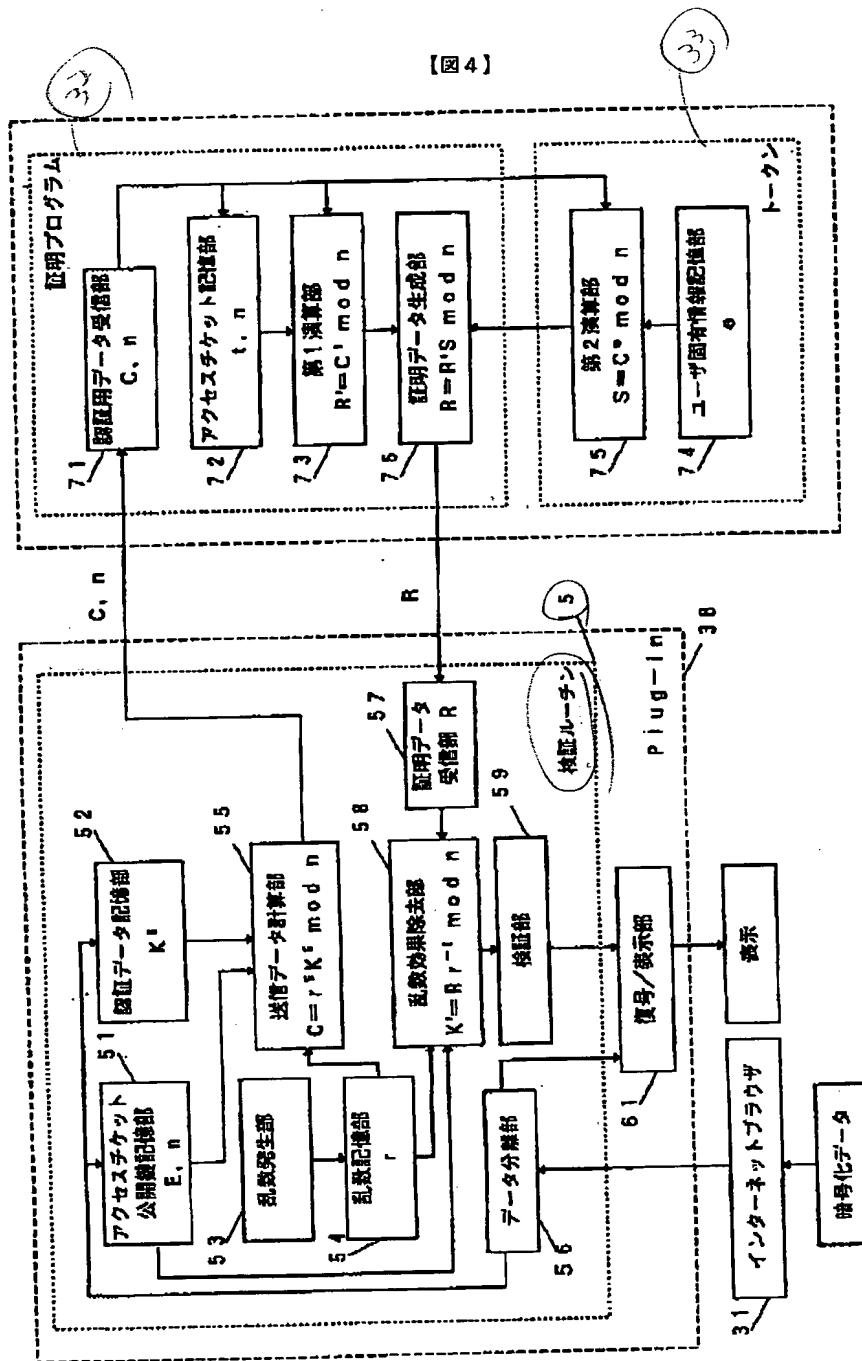


実施例5の構成図

(35)

特開平11-31130

【図4】

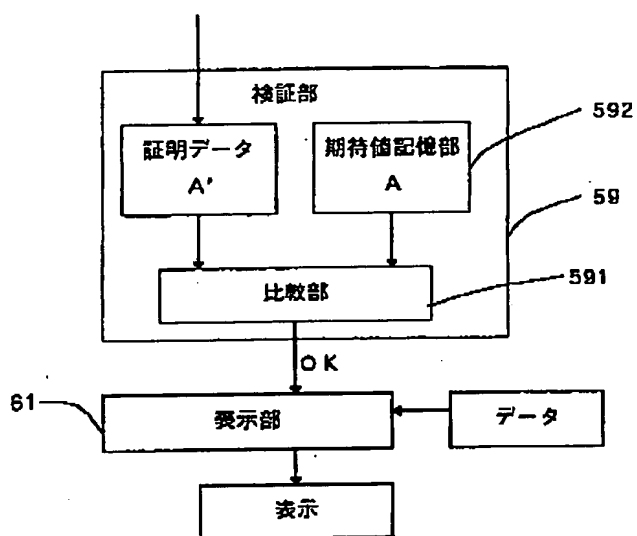


実施例1の詳細な構成例

(36)

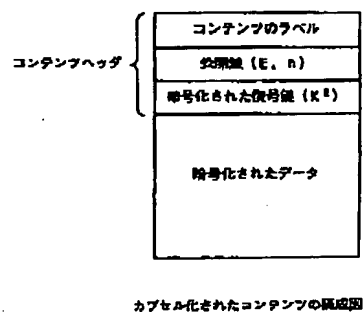
特開平11-31130

【図8】

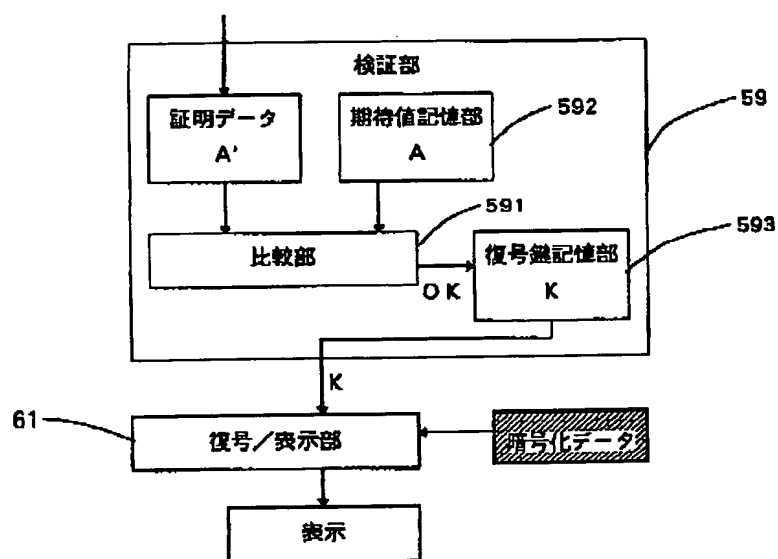


検証部の構成1

【図16】



【図9】

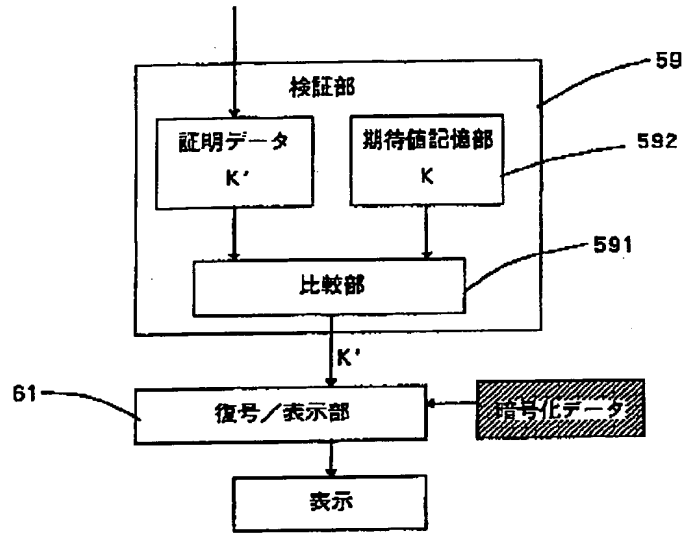


検証部の構成2

(37)

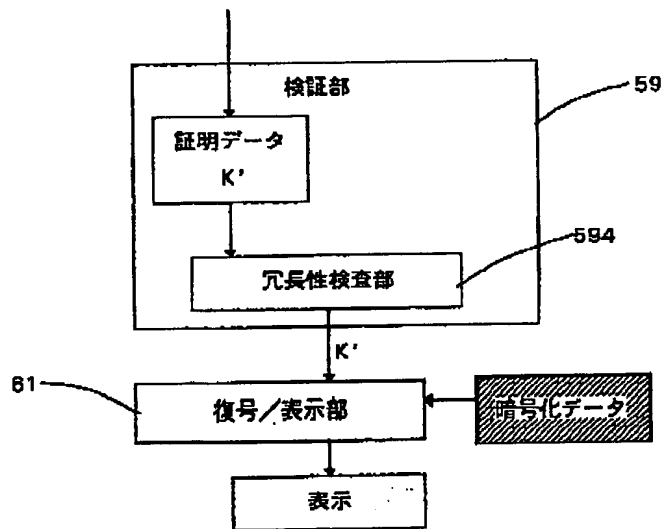
特開平11-31130

【図10】



検証部の構成3

【図11】

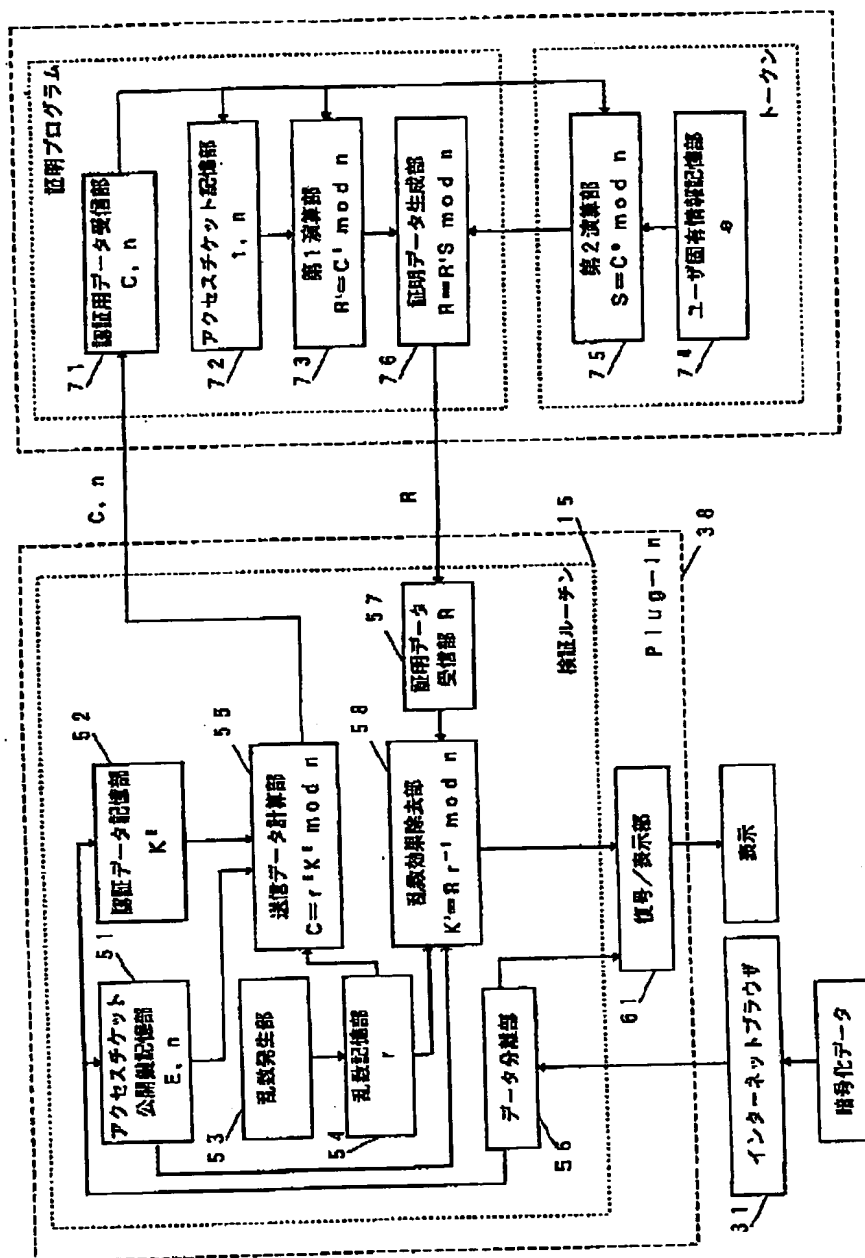


検証部の構成4

(38)

特開平11-31130

【図12】

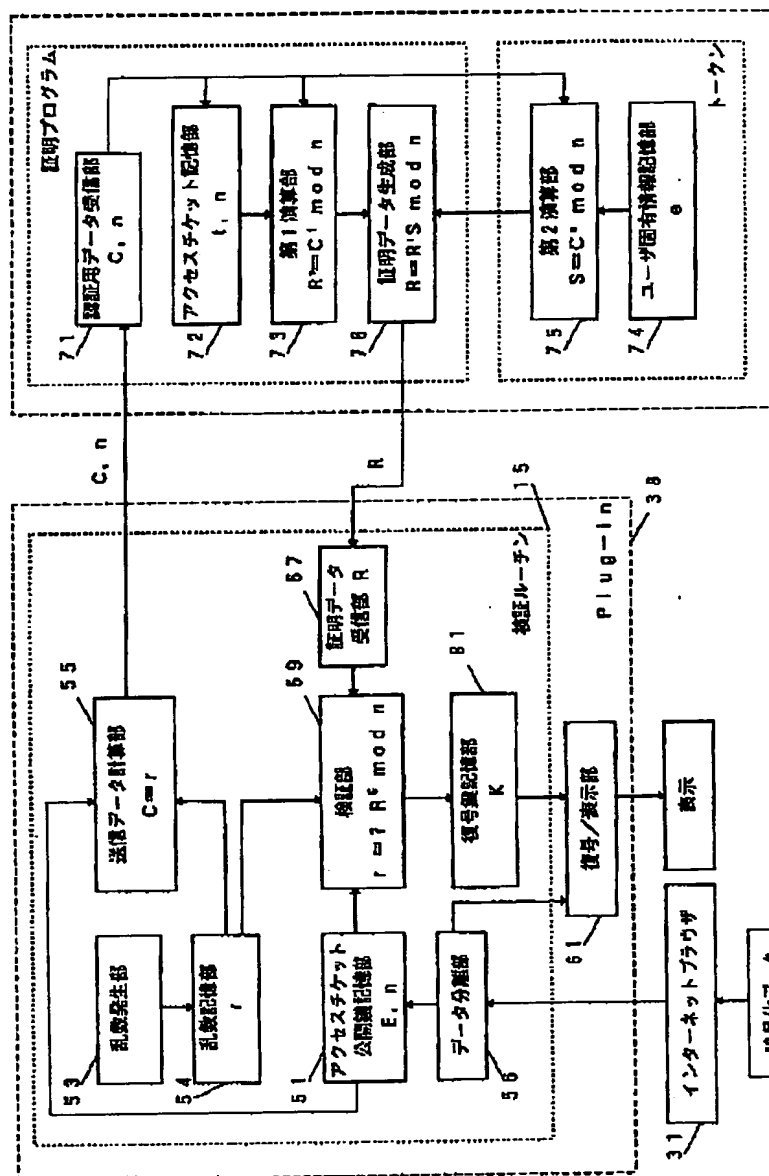


実施例2の構成例

(39)

特開平11-31130

【図13】

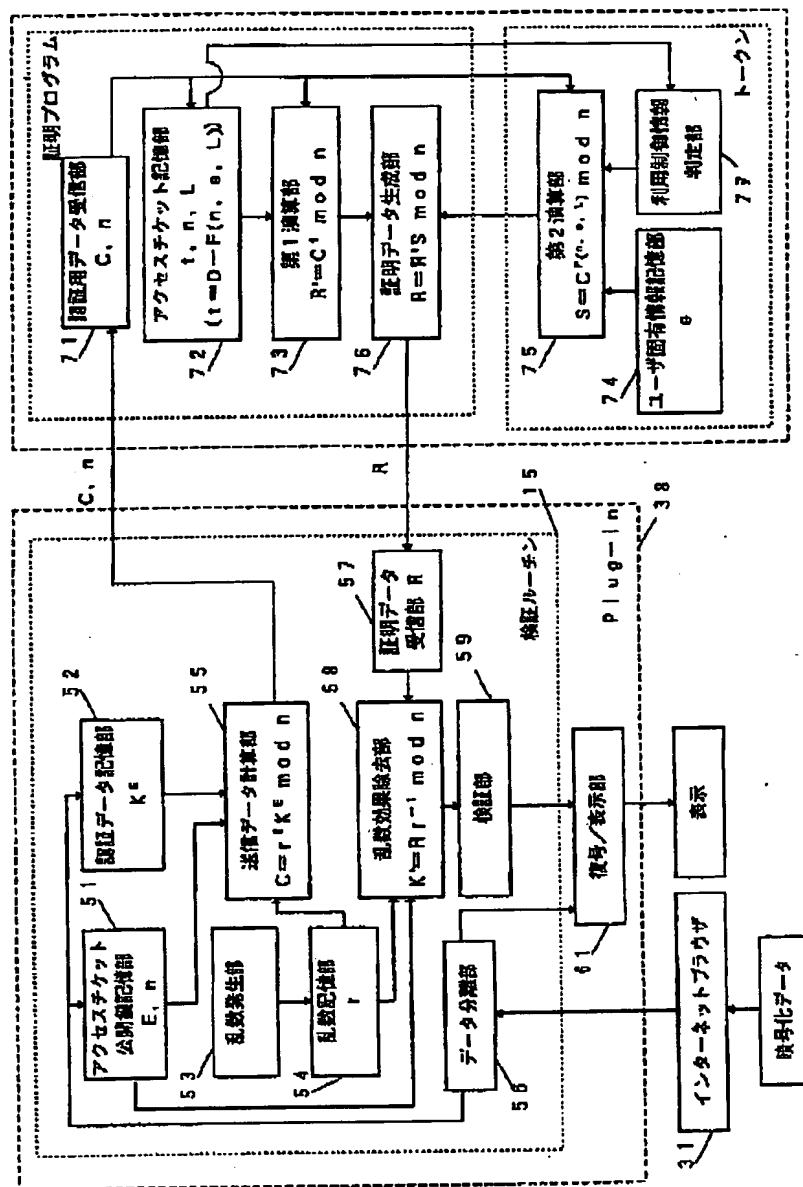


実施例3の構成例

(40)

特開平11-31130

【図14】

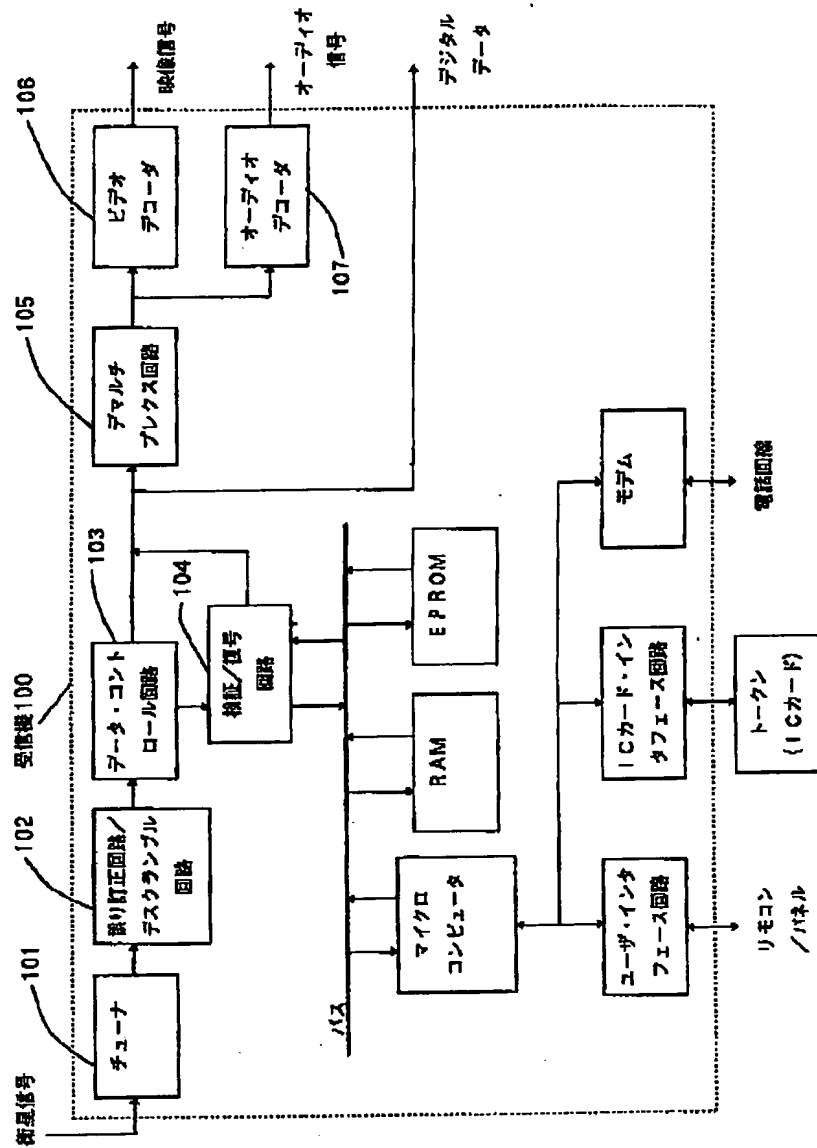


実施例4の構成図

(41)

特開平11-31130

【図17】

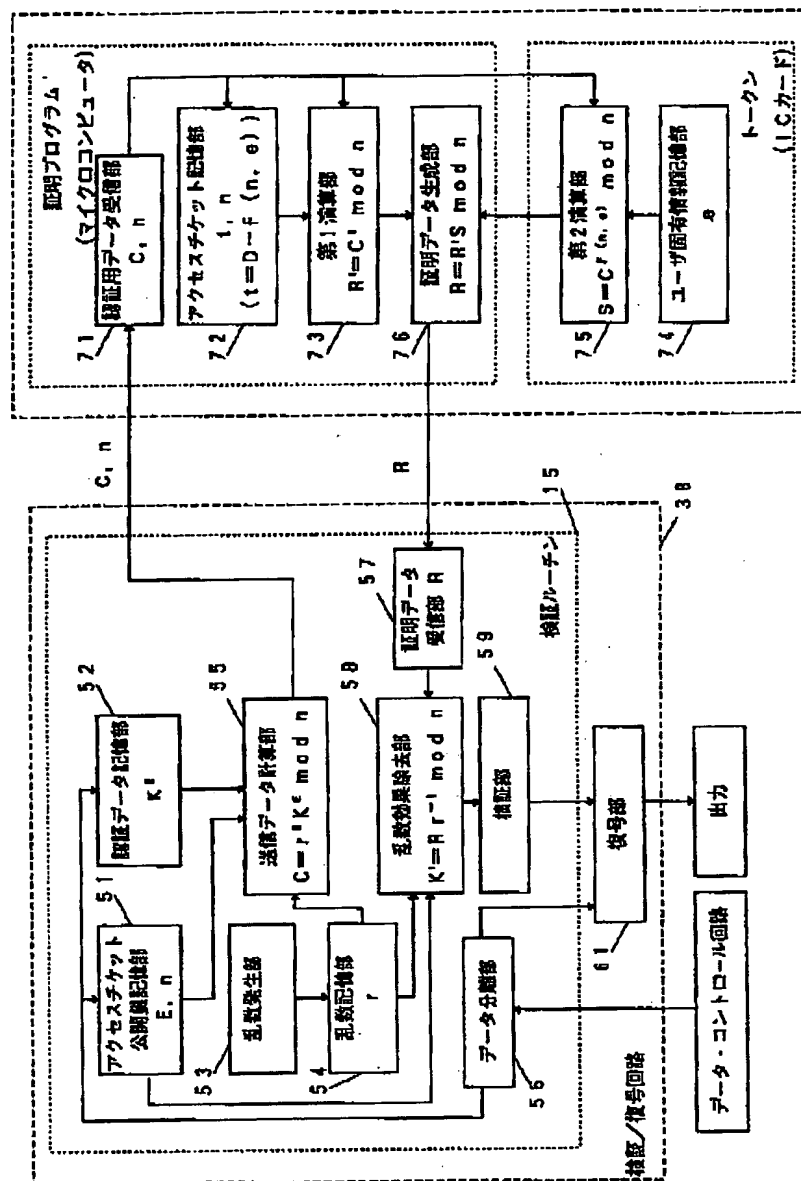


実施例5の構成図

(42)

特開平11-31130

【図18】

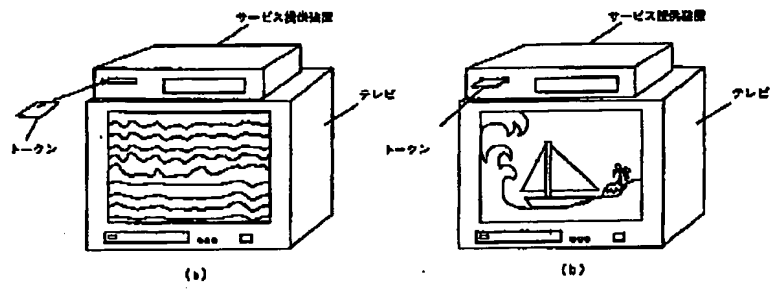


実施例5の構成図

(43)

特開平11-31130

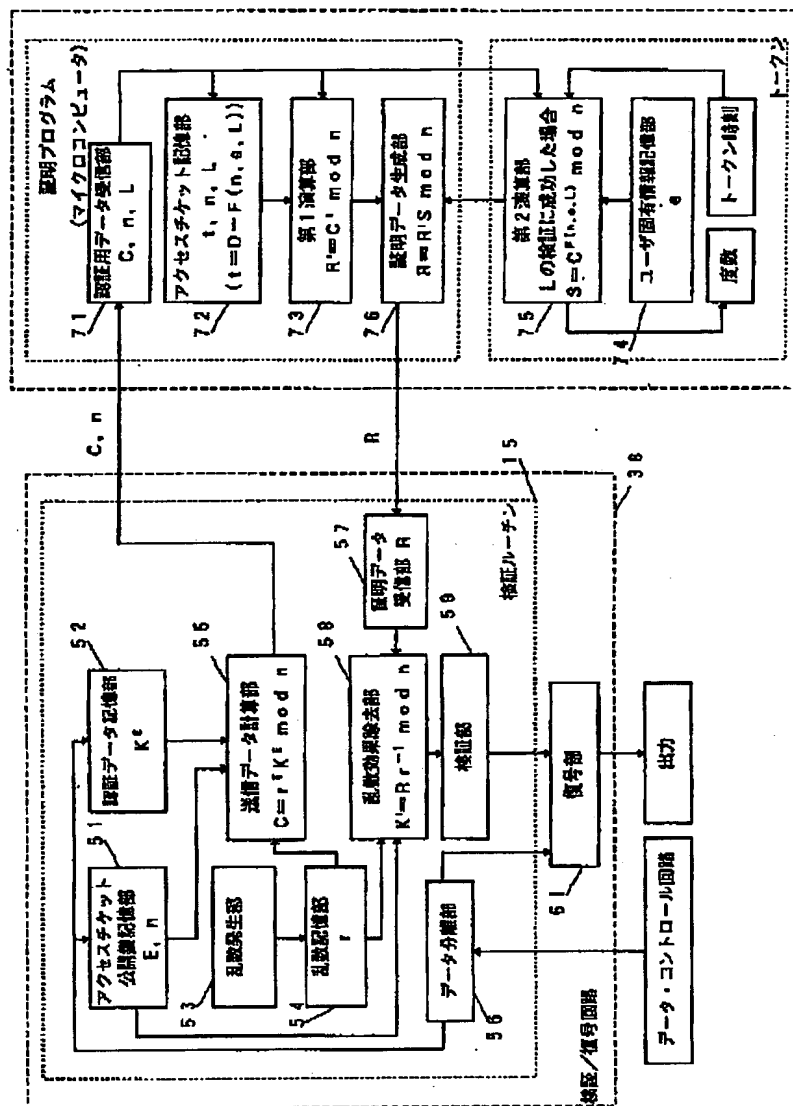
【図19】



(44)

特開平11-31130

【図21】



実施例6の構成図